

2009

Analysis of groups generated by quantum gates

David C. Gajewski
The University of Toledo

Follow this and additional works at: <http://utdr.utoledo.edu/theses-dissertations>

Recommended Citation

Gajewski, David C., "Analysis of groups generated by quantum gates" (2009). *Theses and Dissertations*. 1061.
<http://utdr.utoledo.edu/theses-dissertations/1061>

This Dissertation is brought to you for free and open access by The University of Toledo Digital Repository. It has been accepted for inclusion in Theses and Dissertations by an authorized administrator of The University of Toledo Digital Repository. For more information, please see the repository's [About page](#).

A Dissertation
entitled
Analysis of Groups Generated by Quantum Gates

by
David C Gajewski

As partial fulfillment of the requirements for the
Doctor of Philosophy in Mathematics

Advisor: Dr Paul R Hewitt

College of Graduate Studies

The University of Toledo
August 2009

An Abstract of
Analysis of Groups Generated by Quantum Gates

David C Gajewski

Submitted in partial fulfillment
of the requirements for the
Doctor of Philosophy in Mathematics

The University of Toledo
August 2009

Different forms of computational systems, such as binary computers and Turing Machines, are known to be able to efficiently simulate each other. This is the basis of the Church-Turing Thesis which stipulates that any sufficiently powerful model of computing is equivalent to any other - any algorithm in one model can be translated, in polynomial time, to an equivalent algorithm in another. In 1982 a new form of computation was introduced which is based on the effects of Quantum Mechanics. It is currently unknown if Quantum Computing can be efficiently simulated by a classical computer, and thus might be a more powerful system of computing.

The aim of this dissertation is to study the complexity of quantum computations from the perspective of groups. Two groups will receive extensive study. Each Toffoli group is determined and a minimal generating set for each will be constructed, also the type of simple group created by the direct limit of the Toffoli groups will be determined. The frames of each Pauli group will be analyzed and lead to a different realization of the Clifford Group. Let h be the Hadamard Gate, a purely quantum operator, and let P_{2n} be the collection of permutation matrices of alternating type.

We will see how $\mathrm{SO}_{2n}(\mathbb{Z}[1/2]).\langle H \rangle = \langle (h \otimes I)^\sigma | \sigma \in P_{2n} \rangle$, and that this suggests an algorithm which decomposes a quantum operator into a sequence of basic operators which are purely quantum or purely classical. This metric, and another based on buildings, will be explored.

Contents

Abstract	ii
Contents	iv
1 Computation	1
1.1 Classic Computation	2
1.1.1 Fredkin Operators	6
1.1.2 Toffoli Operators	11
1.1.3 Minimal Generators for the Toffoli Group	14
1.1.4 Infinite Toffoli group	17
1.2 Quantum Computation	20
1.2.1 Classical Gates	24
1.2.2 Quantum Gates	24
1.2.3 Another Generation of the Clifford Group	28
2 Geometry	37
2.1 Analysis of the Coset Geometry	39
2.2 Tensor Products	41

3	Main Theorem	42
3.1	Proof of the Main Theorem	43
3.2	The Main Theorem as an Algorithm	48
3.3	Normalizers	53
4	Quadratic Forms over \mathbb{Q}_2	57
4.1	p -adics	57
4.2	Quadratic Forms	58
4.3	Moving Between Forms	62
A	Appendix	67
A.1	Buildings	67
A.1.1	Coxeter Groups	68
A.1.2	Coxeter Complexes	72
A.1.3	Buildings	75
A.1.4	Buildings over the p -adics	78
A.2	Reduction Modulo p	83
A.3	Source Code	87
	References	96

Index

P_{2N} , 42

T_∞ , 17

$\mathbb{Z}\{1/\sqrt{2}\}$, 42

c_j^i , 6

$f_{j,k}^i$, 6

$o_p(n)$, 58

$t_k^{i,j}$, 11

$w_{n,k}$, 7

binary string, 5

bit weight, 7

Clifford Group, 24

CNot gate, 5

decomposition length, 48

Frame, 28

Fredkin gate, 6

gate, 2

reversible, 4

universal, 3

Hadamard gate, 24

Kegel cover, 18

Kronecker product, 41

Oriflamme Geometry, 78

Pauli gate, 25

Phase gate, 25

q-bit, 22

Toffoli gate, 11

weight of column, matrix, 43

Introduction

One yet unanswered question is whether a quantum calculation can be efficiently simulated on a classical computer. An aim of this paper is to study the complexity of quantum computations from the perspective of groups. Specifically, an algorithm will be shown which decomposes a quantum operator into a sequence of basic operators which are purely quantum or purely classical. Furthermore groundwork will be laid for placing a metric on calculations by way of a building. A given metric may lead to a new type of complexity to consider for a quantum algorithm.

This paper also asks new questions of the standard building blocks for both classical and quantum computing. The new results are: the Main Theorem, analyzing the Fredkin Group (Theorem 1.1.1), analyzing the Toffoli Group (Theorems 1.1.4, 1.1.7, and 1.1.9), and Theorems 1.2.3 and 1.2.4 related to frames of the Pauli Groups. Even when the result is already known, the proofs presented here are original.

Chapter 1

Computation

Data and information are the building blocks of knowledge. First mathematically quantified by Claude Shannon in the 1940's, information is often used to find further information. Computation is the act of processing information. Algorithms are the step-by-step procedures which transform given data into new information. They can be as familiar as the steps for long division, or as abstract as the methods car navigation systems use to find an optimal route to a destination. Many important computations are the algorithms used by computers to process data.

Before the advent of computers, researchers noticed that different models of computation were able to simulate all of the others. This idea was dubbed the Church-Turing Thesis, named after the distinguished researchers Alonzo Church and Alan Turing. A refined version of this idea is the strong Church-Turing Thesis, which states that “Any algorithmic process can be simulated efficiently using a Turing machine.” It was not a mathematical theorem, but a series of observations that any rich enough system designed to perform computations was no better than any other.

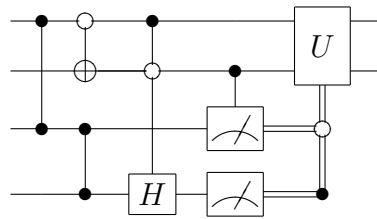
These systems included such things as Turing machines, lambda calculus, and automata even including Conway's Game of Life, and it was seen that they could all *efficiently* simulate the others. For instance the class of all algorithms which could be run in time which is proportional to the size of the input raised to some power (also known as polynomial time) would stay in that class of algorithms when being simulated by another machine.

Currently there is no model of computation which has been proved to be more powerful than Turing Machines (or its equivalents), but people are still curious as to whether there might be. Newer computational models being studied include analog computers, DNA computers, and the focus of this paper, quantum computers. Although there is no definitive proof, it appears that quantum computers may indeed be more powerful than the classical variety.

1.1 Classic Computation

One good model of computation is the digital computer. The information being acted upon is called data and the smallest quantity of information is called a bit, which is either 0 or 1. These bits are stored electronically. The most basic form of computation here is an electrical circuit called a gate, which takes as an input one or more bits and outputs one or more bits. For example, a NOT gate takes a bit and outputs the opposite value of that bit. Also, an AND gate takes two bits as input and outputs a single bit which has the value 1 if and only if both inputs had value 1. Other examples include OR, XOR, NAND, and NOR.

To visually represent a gate or series of gates acting on a bit, one can draw a wire diagram. A wire diagram consists of wires and gates. The wires represent physical wires carrying a bit as an electric signal. Gates are represented in the wire diagram by various shapes such as squares or triangles, with the appropriate number of wires entering the gate as inputs and similarly leaving for outputs. A wire diagram is to be read left-to-right, and one can think of a vertical slice through the diagram as being a state of the system as time progresses. Thus, the gates on the far left are activated first, and those on the far right, last.



The above is an example of a generic wire diagram. Some gates are represented with boxes, and others are shown with vertical wires joining some of the horizontal wires. The former will usually be a type of gate which acts on a single wire, and the latter will represent common gates which act on multiple wires.

There are infinitely many gates that one could construct, but it turns out that a finite number of them can be combined in various ways to give the same results on the same input. Any set of gates which do this is called a set of universal gates. For instance, the NAND and NOR gates (which can be thought of as AND followed by NOT and OR followed by NOT) turn out to be universal for all gates found on a computer. As an example, a circuit could be made completely out of these gates to

compute addition on bounded integers via their binary representation. Having a set of universal gates allows one to study this particular computing model efficiently.

A gate is said to be reversible if there is another gate (or series of gates) which acts on the output and returns the original input. Notice that the reverse of a reversible gate is itself reversible. This requires that the number of outputs of a gate must be the same as the number of inputs, since otherwise the gate would not be either injective or onto all possible states. Since a reversible gate has the same number of inputs and outputs, information is neither created (which requires more electrical energy) nor destroyed (which generates heat). For this reason, reversible computing is finding its way into modern computer circuits and CPUs.

Any classical gate can be turned into a reversible gate. If a gate has n inputs and m outputs, start with an input of length $n + m$ where the original input is on the first n and 0's fill the remainder. These are called ancillary bits. The output of the gate will be the original input, followed by the m output bits for the desired gate. The gate acting on $m + n$ long inputs with the last m bits not all 0 is undefined, and so they can be mapped bijectively to the unused $n + m$ bit outcomes. In this way the new gate is a permutation on all binary strings of length $n + m$. Notice that a permutation realizes the reordering of output wires of one gate as the input of another. The output of the first gate consists of the output, copied over ancillary bits filled with 0, and junk bits which allowed the computation to be a permutation. Each gate after the first are constructed in a similar manner in such a way that they respect the results of valid zero-padded inputs pushed through the previous gates. Thus, if the number of input plus output bits is bounded, any reversible gate can be represented

as a permutation on binary strings of bounded length. Composition of gates is thus the composition of permutation elements. This shows that the full symmetric group contains these reversible gates, and can be thought of as the universe for gates of this form. As computing and reversible computing are equivalent in power as models of computation, we will henceforth take the viewpoint of reversible computation. As one might expect, reversible universal gates are even more interesting to study, as collections of gates now generate permutation groups.

In classical computers, one has gates acting on, say n binary inputs. It is instructive to see how such gates act on the 2^n different inputs as permutations on that set. For convenience, we identify the binary string $b_{n-1} \dots b_0$ with its base two expansion $\sum_{i=0}^{n-1} 2^i b_i$. Then the study of classical computations on n bits is identified with its permutations on the integers $0, \dots, 2^n - 1$.

When analyzing the individual bits of a binary string, we often describe a bit being set or cleared.

Definition 1. *The i^{th} bit being set means $b_i = 1$ and being clear means that $b_i = 0$.*

Definition 2. *The binary string where each b_i is clear is denoted $\bar{0}$ and the binary string where each is set is $\bar{1}$.*

There are three reversible classical gates: the controlled not (CNot), Fredkin, and Toffoli. We will see that the Toffoli gate is universal and thus can be used to simulate the other two. Hence any classical computation on a fixed number of bits can be achieved by applications of the Toffoli gate on all possible wire combinations.

The simplest of the reversible classical gates is the CNot gate, denoted c_j^i . It acts

on two inputs - one of the bits is called the control (bit i) and the other the target (bit j). The value of the target bit is flipped if and only if the control bit is set. Note that the CNot gate applied twice is the identity, and thus is an order two operator,

$$\tilde{b} = c_j^i(b), \quad \text{where} \quad \tilde{b}_m = \begin{cases} 1 & \text{if } m = j, b_m = 0, \text{ and } b_i = 1, \\ 0 & \text{if } m = j, b_m = 1, \text{ and } b_i = 1, \\ b_m & \text{otherwise} \end{cases}$$

As an example suppose that a CNot gate is acting on a system with two bits, then we can identify every state of the system with the integers 0 through 3. The gate which uses bit 0 as control (with bit 1 as target) acts as the permutation (1 3), and the gate which uses bit 1 as control acts as the permutation (2 3).

1.1.1 Fredkin Operators

The Fredkin operators are classical operators which can be viewed as controlled swaps. The operator $f_{j,k}^i$ swaps the j^{th} and k^{th} bits when the i^{th} bit is set. It is required that i, j , and k are distinct.

$$\tilde{b} = f_{j,k}^i(b), \quad \text{where} \quad \tilde{b}_m = \begin{cases} b_k & \text{if } m = j \text{ and } b_i = 1, \\ b_j & \text{if } m = k \text{ and } b_i = 1, \\ b_m & \text{otherwise} \end{cases}$$

The group generated by all Fredkin operators on n bits is denoted F_n , so that $F_n = \langle f_{j,k}^i | i, j, k \text{ distinct and } \leq n \rangle$. The distinctness implies that $n \geq 3$ to have F_n

defined.

Definition 3. *The bit weight of a binary string (or number) is the number of 1 bits it contains.*

In this way, all binary inputs of n bits can be partitioned into sets by their weight. Let $w_{n,k} = \{b_{n-1} \dots b_0 \mid \text{weight}(b_{n-1} \dots b_0) = k\}$. For example, $w_{2,0} = \{00\}$, $w_{2,1} = \{10, 01\}$, and $w_{2,2} = \{11\}$. Or, by using the bijection between binary strings of length n and the integers $0, \dots, 2^n - 1$, $w_{2,0} = \{0\}$, $w_{2,1} = \{1, 2\}$, and $w_{2,2} = \{3\}$.

Notice that by the definition of the Fredkin operators, swapping bits does not change the weight, so that $\text{weight}(f_{j,k}^i(b)) = \text{weight}(b)$. Hence each orbit of F_n is contained in $w_{n,k}$ for some k .

The orbits of F_n are precisely $w_{n,0}, w_{n,2}, \dots, w_{n,n}$, and the individual elements in $w_{n,1}$ since both $w_{n,0}$ and $w_{n,n}$ are singleton sets. For a binary string of weight 1, either $b_i = 0$ or $b_i = 1$ and $b_j = b_k = 0$. In either case, $f_{j,k}^i$ acts trivially and thus so does F_n .

Theorem 1.1.1. *Let $A_n = \text{Alt}(w_{n,2}) \times \dots \times \text{Alt}(w_{n,n-1})$. The derived subgroup of each Fredkin group, F_n , is A_n and is of index 2.*

Proof. Let $B_n = \langle f_{j,k}^i f_{s,t}^r \mid i, j, k \text{ are distinct and so are } r, s, t \rangle$, the subgroup generated by products of pairs of generators for F_n . The proof will show that $B_n = A_n$ and then that $F_n' = A_n$. Pick any generator and call it f_0 , for example f_0 could be $f_{1,2}^0$. Now f_0 acting on binary strings of weight 2 interchanges precisely two of them. The example generator is a permutation between $0 \dots 011$ and $0 \dots 101$. Hence it is a transposition over $w_{n,2}$, and so $f_0 \notin A_n$ since it is odd. The cycle structure over each weight space

is the same for each $f_{j,k}^i$. Thus each generator of B_n is an even permutation over each $w_{n,i}$ and $B_n \subseteq A_n$.

If x is any member of F_n , x can be written as a product of k generators. If k is even, then $x \in B_n$ by construction. If k is odd, then $x = f_1 \cdots f_k = f_0 f_0 f_1 \cdots f_k \in f_0 B_n$. Only two cosets for B_n in F_n gives that the group F_n has a normal subgroup of index 2 contained in A_n .

For F_3 we have $f_{0,1}^2 = (5\ 6)$ and $f_{0,2}^1 = (3\ 6)$ so that $F_3 = \text{Sym}(w_{3,2})$. It is then apparent that $B_3 = \text{Alt}(w_{3,2})$.

For $n > 3$ we use induction. Suppose $B_{n-1} = \text{Alt}(w_{n-1,2}) \times \cdots \times \text{Alt}(w_{n-1,n-2})$. Fix a weight w_0 . Take any element f of B_{n-1} which fixes elements of weight $w \neq w_0$ and moves elements of weight w_0 . Then f , as defined by its Fredkin generators, also acts on binary strings of length n . Here, f moves twice as many binary strings as before - a copy of two equal cycle structures with one collection adding a 0 bit and the other a 1 bit. Thus now f as seen as an element of F_n moves elements of weight w_0 and $w_0 + 1$.

We first show that the collection of elements from $\text{Alt}(w_{n-1,n-2})$ in B_{n-1} , taken with every permutation of the bits, generate $\text{Alt}(w_{n,n-2}) \times \text{Alt}(w_{n,n-1})$. Consider the 3-cycles of $\text{Alt}(w_{n-1,n-2})$ as acting on n bits, so each are now pairs of 3-cycles. If σ is any permutation of the n bits $\{0, 1, \dots, n-1\}$, then defining $\sigma \cdot f_{i,j}^k = f_{\sigma(i),\sigma(j)}^{\sigma(k)}$ shows $\sigma \cdot f$ permutes the bits for the 3-cycle pairs. The group generated by such elements is transitive on $w_{n,n-2}$ and $w_{n,n-1}$. This is since the collection of elements of weight $n-2$ (or $n-1$) are already known to be in the same orbit, and a 3-cycle pair can be found to join any same weighted element with the opposite parity for the last bit.

Just take a bit permutation σ which alters the parity of the last bit, take two elements of the same weight (and any three of the other weight) for which 0 (resp. 1) would get moved into the last position by σ and the permuted 3-cycle pair has the desired effect.

The group which is generated has homomorphisms onto each of the permutation groups of its orbits. It is well known that 3-cycles which are transitive on a set generate the alternating group on that set. With two orbits, the kernel is a group which acts only on the other orbit. The intersection of these subgroups is trivial, so considering the product of the homomorphisms shows that the group generated by these 3-cycle pairs is embedded as a subgroup of $\text{Alt}(w_{n,n-2}) \times \text{Alt}(w_{n,n-1})$. The homomorphisms show these distinct, simple alternating groups (and $\text{Alt}(4)$) comprise the simple factors of each group. Hence the group generated is $\text{Alt}(w_{n,n-2}) \times \text{Alt}(w_{n,n-1})$, as the kernels must be the full alternating groups.

Finally we use the higher weight alternating subgroups to produce the lower weight ones. Suppose we have generated $\text{Alt}(w_{n,k+1}) \times \cdots \times \text{Alt}(w_{n,n-1})$. Then consider three cycles taken from A_{n-1} (and their bit permutations) which operate on elements of weight k . Then on n bits it is a pair of 3-cycles, one of which operates on elements of weight k and the other on $k+1$. From the already generated alternating product we have the inverse of the part acting on weight $k+1$ elements. Thus we have 3-cycles only moving elements of weight k and this collection is similarly transitive on $w_{n,k}$. Hereby we are able to append $\text{Alt}(w_{n,k})$ to the direct product and eventually generate A_n .

For $n > 4$, the alternating subgroups of A_n are simple and so the derived group

of A_n is A_n . Considering commutators of such F_n one sees that when a distinguished element f_0 which generates the non-identity coset is needed in a product, it appears in pairs, giving an even number of Fredkin generators. So $F'_n \subseteq B_n = A_n$, and thus $F'_n = A_n$. Since F_3 is isomorphic to $\text{Sym}(3)$, $F'_3 = A_3$. Finally one can check that $F'_4 = A_4$. Therefore the derived group of F_n is A_n , and it is of index 2 in the full group, F_n . \square

Proposition 1.1.2. *F_n is generated by the direct product of alternating groups over the orbits $w_{n,k}$ and a single element t . This element t is a product of transpositions, with a transposition on those orbits $w_{n,k}$ for which $\binom{n-3}{k-2}$ is odd.*

Proof. Let $t_{n,k}$ be the number of transpositions a single generator defines on $w_{n,k}$. $t_{n,k}$ will be shown to be $\binom{n-3}{k-2}$. As each Fredkin generator has the same cycle structure over the orbits, one only needs to consider one of them. The labeling is inconsequential as each generator relies on three wires. For the $n = 3$ case, k must be 2 and each Fredkin generator is a transposition. So $t_{3,2} = 1$, with $t_{3,k} = 0$ otherwise. When a lone transposition in F_n is embedded in F_{n+1} it becomes a pair of transpositions. One transposition affects binary strings of the same weight as before, where the added bit is 0, and the other moves binary strings of one weight higher. So transpositions effecting $w_{n+1,k}$ in F_{n+1} came from transpositions effecting $w_{n,k-1}$ and $w_{n,k}$ in F_n . Hence, when considering at the transpositions of a single Fredkin generator, $t_{n+1,k} = t_{n,k-1} + t_{n,k}$. This is just the binomial recurrence relation. Shifting this Pascal's Triangle to be rooted at $n = 3$ $k = 2$ gives the desired result. \square

Thus, fixing n , any element x in F_n has a standard presentation. The portion of

the permutation of x over $w_{n,k}$ when $\binom{n-3}{k-2}$ is even for each k is an even permutation (possibly the identity). However, x has either an even permutation or an odd permutation simultaneously over each $w_{n,k}$ for all those k for which $\binom{n-3}{k-2}$ is odd.

One can also observe that the Fredkin generators are conjugate in each Fredkin group. It is true for F_3 as it is a symmetric group. Inductively, in F_{n+1} Fredkin generators which ignore the same wire are all conjugate. These collections overlap, and a chain of conjugation can be made from one generator to any other.

1.1.2 Toffoli Operators

The Toffoli operators are classical operators which can be viewed as controlled-controlled nots. A controlled not operator is a two bit operator which performs the NOT operation on the first bit only if the second bit, the control bit, is set. A controlled-controlled not is a controlled not operator with an additional control bit, which means that both control bits must be set for the NOT operation to be performed. The operator $t_k^{i,j}$ flips the k^{th} bit if both the i^{th} and j^{th} bits are set. As with the Fredkin operators, it is required that $i, j,$ and k are distinct.

$$\tilde{b} = t_k^{i,j}(b), \quad \text{where} \quad \tilde{b}_m = \begin{cases} 1 & \text{if } m = k, b_m = 0, \text{ and } b_i = b_j = 1, \\ 0 & \text{if } m = k, b_m = 1, \text{ and } b_i = b_j = 1, \\ b_m & \text{otherwise} \end{cases}$$

The group generated by all Toffoli operators on n bits is denoted T_n , so that $T_n = \langle t_k^{i,j} | i, j, k \text{ distinct and } \leq n \rangle$. The distinctness implies that $n \geq 3$ to have T_n

defined. We have that $F_n < T_n$ as $f_{j,k}^i = t_k^{i,j} t_j^{i,k} t_k^{i,j}$ (note b_i must be 1 for any effect, and then consider the 4 cases for b_i, b_j).

The orbits of T_n are $\cup_{k=2}^n w_{n,k}$, $w_{n,0}$ and the individual elements in $w_{n,1}$. Notice that T_n only preserves weights when that weight is 0 or 1. In particular, we see that $w_{n,0} \cup w_{n,1}$ are the only fixed points for T_n . From now on, we only consider T_n acting on binary strings of weight 2 or higher. Recall that by $\bar{1}$, we mean the binary string of all 1's.

Lemma 1.1.3. *T_n is n -transitive. Furthermore, the n point stabilizer is fixed-point free on the remaining points for $n \geq 4$.*

Proof. Let b be a binary string of weight two or higher. It has positions i and j such that $b_i = b_j = 1$. Let $\{k_1, k_2, \dots, k_m\}$ be the (possibly empty) set of positions in the binary string where b_k is 0. Then either $b = \bar{1}$ or $t_{k_1}^{i,j} t_{k_2}^{i,j} \dots t_{k_m}^{i,j}(b) = \bar{1}$. This shows T_n is transitive.

Suppose that T_n has been shown to be $(p-1)$ -transitive, with $p \leq n-1$. Define $p-1$ binary strings b^1, b^2, \dots, b^{p-1} , where $b_0^q = b_q^q = 1$ and all other bits are 0 for q in $1, 2, \dots, p-1$. Let b be a binary string of weight 2 or more. If it has weight greater than 2, then it has positions $i, j > 1$ such that $b_i = b_j = 1$. Thus $t_k^{i,j}(b^q) = b^q$ for each k and q as either the i^{th} or j^{th} position must be zero in b^q . Otherwise, $b \neq b^q$ for any q , so it has set positions i and j and similarly $t_k^{i,j}(b^q) = b^q$ for each k and q . Let $\{k_1, k_2, \dots, k_m\}$ be the (possibly empty) set of positions in the binary string where b_k is 0. Then either $b = \bar{1}$ or $t_{k_1}^{i,j} t_{k_2}^{i,j} \dots t_{k_m}^{i,j}(b) = \bar{1}$. We also have $t_{k_1}^{i,j} t_{k_2}^{i,j} \dots t_{k_m}^{i,j}(b^q) = b^q$ for each q . Hence T_n is p -transitive, and thus 2- through n - transitive.

Lastly, we fix n binary strings b^1, b^2, \dots, b^{n-1} , and $\bar{1}$. We set aside as special $\bar{1}^0 = t_0^{1,2}(\bar{1})$, which has each bit set except the 0th. If b is a binary string of weight 2 or more such that b is not $\bar{1}^0$, then b has a zero bit at b_k for some $k > 0$. Also, b has set bits at $i, j > 0$. Consider $t = t_i^{k,j} t_k^{i,j} t_i^{k,j}$. We have that $t(b)_i = 0$, $t(b)_k = 1$, and $t(\bar{1}) = \bar{1}$. It is straightforward that t fixes each b^q . For the case $b = \bar{1}^0$, $t = t_0^{1,2} (t_0^{2,3} t_3^{0,1})^2$ does the job - $t(b)_3 = 0$. We have shown that no further points are stabilized within this stabilizer. The result holds as the group is n -transitive. \square

Theorem 1.1.4. $T_4 \cong \text{Sym}(4)$. For $n \geq 4$, T_n acts as the full alternating group, $\text{Alt}(2^n - n - 1)$, on the $2^n - n - 1$ non-fixed points.

Proof. It is obvious that $T_3 = \langle (3\ 7), (5\ 7), (6\ 7) \rangle \cong \text{Sym}(4)$. For the other groups, our goal is to find a 3-cycle. Once one is obtained, having 3-transitivity gives us all 3-cycles and that $\text{Alt}(2^n - n - 1) \subseteq T_n$. Each $t_k^{i,j}$ is a product of 2^{n-3} disjoint transpositions - it moves each binary string with positions i and j set with order 2. The generators all being even permutations for $n > 3$ gives us the reverse inclusion.

In T_4 a generator $t_k^{i,j}$ has the cycle structure $(a\ b)(c\ d)$. By 4-transitivity, there is a permutation σ such that $[(a\ b)(c\ d)]^\sigma = (a\ b)(c\ e)$. Their product is a 3-cycle, $(a\ b)(c\ d)[(a\ b)(c\ d)]^\sigma = (e\ d\ c)$.

The general case is handled by induction. If T_{n-1} has a 3-cycle $(a\ b\ c)$, then $(a\ b\ c)(a+2^{n-1}\ b+2^{n-1}\ c+2^{n-1})$ is an element of T_n . Let's call it $(a\ b\ c)(r\ s\ t)$. If $n \geq 6$, then as T_n is 6-transitive, there is a $\sigma \in T_n$ such that $[(a\ b\ c)(r\ s\ t)]^\sigma = (d\ b\ a)(t\ s\ r)$. Their product is $(a\ d\ c)$, as two of the 3-cycles are inverses.

For $n = 5$ we can only move 5 elements as we like. So, fixing a permutation σ for

elements except for a , we get $[(a\ b\ c)(r\ s\ t)]^\sigma = (x\ b\ a)(t\ s\ r)$, where x is unknown. If $x = c$, pick τ in the $\{a, b, r, s, t\}$ stabilizer which moves c (which exists by Lemma 1.1.3). Replace σ with $\sigma\tau$, and the product of the pair of 3-cycles with its permutation is $(a\ x\ c)$, since $x \neq c$. \square

1.1.3 Minimal Generators for the Toffoli Group

Our aim in this subsection is to find a subset of the generating set $\{t_{i,j}^k\}$ which minimally generates a Toffoli group. The number of generators $t_{i,j}^k$ is $n(n-1)(n-2)$, as the indicies must be distinct. One already has that $t_{i,j}^k = t_{j,i}^k$, which shrinks the necessary number of required generators by half. Another necessary condition required by a minimal subset of Toffoli generators is that they must move each element of weight 2. An element of weight 2 can be represented by $2^i + 2^j$, and the only generators which move such an element are of the form $t_{i,j}^k$, where k is arbitrary. Note that the resulting binary string now has weight 3. Conversely, every generator moves only one element of weight 2, the set bits being the same as the control bits of the generator. Thus, a minimal generating set which satisfies this weak necessary condition is in 1-1 correspondence with the elements of weight 2. There are $\frac{n(n-1)}{2}$ such elements, and so this is also a lower bound for the number of minimal generators of the Toffoli group.

Lemma 1.1.5. *A subset of Toffoli generators on n bits is transitive on the set of elements not of weight 0 or 1 if and only if for every element not of maximal weight there is a generator which increases the weight of that element by 1.*

Proof. Recall the binary string of weight n , which is composed of all 1's, is denoted $\bar{1}$.

Suppose that for every element other than $\bar{1}$, there is a generator which increases its weight. Then given a binary string x of length n there is a sequence $\{s_1, s_2, \dots, s_k\}$ such that $\{x, s_1 \cdot x, s_2 s_1 \cdot x, \dots, g_x \cdot x = s_k \cdots s_2 s_1 \cdot x\}$ are increasing in weight and $g_x \cdot x = \bar{1}$. Given two distinct elements x and y , repeat the above if one of them is $\bar{1}$. Otherwise use the construction to obtain g_x and g_y such that $g_x \cdot x = \bar{1} = g_y \cdot y$ and then $y = g_y^{-1} g_x \cdot x$ and hence the subset forms a transitive group.

Suppose the subset of generators is transitive, and pick a binary string x of weight between 2 and $n-1$. Then there is a group element, written as a product of generators, which moves x to $\bar{1}$. In this product of generators, there is a generator t which first sets a bit outside of the originally set bits. The control bits of t must lie in the originally set bits of the binary string, as it is the first to set something outside of that set, and so $x \cdot t$ has a weight 1 higher than x . \square

Now we construct a generating set of size $\frac{n(n-1)}{2}$ which will generate a transitive group. For n bits, where i and j are between 0 and $n-1$, define $k(i, j)$ as follows:

$$k(i, j) = \begin{cases} 0 & \text{if } i \neq 0 \text{ and } j \neq 0, \\ j + 1 & \text{if } i = 0 \text{ and } j \neq n - 1, \\ i + 1 & \text{if } j = 0 \text{ and } i \neq n - 1, \\ 1 & \text{if } i = 0 \text{ and } j = n - 1 \text{ or if } j = 0 \text{ and } i = n - 1 \end{cases}$$

This performs a NOT operation on 0 if i and j are different from 0. If one index is 0, it performs a NOT operation on a successor of the other index (taken circularly and ignoring 0). Let our generating set be $T'_n = \{t_{i,j}^{k(i,j)} | i < j < n\}$. We will show that T'_n is a minimal generating set. Given any binary string x which is not $\bar{1}$, if bit 0 is set then there is a bit j which is set but the successor of j is not. As the weight of the string is at least 2, if 0 is not set then there is a pair i and j which are set. Then $t_{i,j}^{k(i,j)} \cdot x$ has a higher weight than x . As x was arbitrary, and by Lemma 1.1.5, the group generated by the selected generators is transitive.

Lemma 1.1.6. $t_{i,j}^k = t_{i,m}^k t_{i,j}^m t_{i,m}^k t_{i,j}^m$

Proof. Notice that this also says $t_{i,j}^k = (t_{i,m}^k t_{i,j}^m)^2$ and $t_{i,j}^k = [t_{i,m}^k, t_{i,j}^m]$. If bit i is clear, both sides affect nothing. Now assume that i is set. If bit j is clear, the left hand side is the identity, and the right hand side is $(t_{i,m}^k)^2$ which is also the identity. Now assume that bit j is also set.

If bit m is clear, then $t_{i,j}^m$ sets it. So $t_{i,m}^k t_{i,j}^m$ sets m and performs the NOT operation on k . Thus $t_{i,j}^m t_{i,m}^k t_{i,j}^m$ preserves m and flips bit k . Thus the right hand side can be seen to preserve m and flip k , and thus is the operation $t_{i,j}^k$. A similar argument shows that when bit m is set that both listed operations have the same exact effect. \square

Theorem 1.1.7. *The group over $n > 3$ bits generated by T'_n is the Toffoli group T_n and T'_n is a minimal generating set.*

Proof. First we note that the generators in the set T'_n are contained in T'_{n+1} save for $t_{0,n}^1$. However, $t_{0,n}^1 = t_{0,n+1}^1 t_{0,n}^{n+1} t_{0,n+1}^1 t_{0,n}^{n+1}$ by Lemma 1.1.6. Thus T'_n is contained in the generated group $\langle T'_{n+1} \rangle$.

Starting at the base of induction, $T'_3 = \{t_{0,1}^2, t_{0,2}^1, t_{1,2}^0\}$. Knowing that $t_{i,j}^k = t_{j,i}^k$, we see that $\langle T'_3 \rangle = T_3$, as the Toffoli group is generated by all Toffoli generators $t_{i,j}^k$. Now, assume that $\langle T'_n \rangle = T_n$. We have that $T_n = \langle T'_n \rangle \subset \langle T'_{n+1} \rangle$, and so $\langle T'_{n+1} \rangle$ contains the Toffoli generators of T_n . We wish to show that $\langle T'_{n+1} \rangle$ contains the rest of the Toffoli generators - those involving bit $n + 1$.

For i, j, k, m being distinct and neither 0 nor $n + 1$, Lemma 1.1.6 gives that (each line assuming the previously generated):

$$t_{0,n+1}^k = t_{0,m}^k t_{0,n+1}^m t_{0,m}^k t_{0,n+1}^m \quad (1.1)$$

$$t_{0,j}^{n+1} = t_{0,n}^{n+1} t_{0,j}^n t_{0,n}^{n+1} t_{0,j}^n \quad (1.2)$$

$$t_{i,j}^{n+1} = t_{i,0}^{n+1} t_{i,j}^0 t_{i,0}^{n+1} t_{i,j}^0 \quad (1.3)$$

$$t_{n+1,b}^1 = t_{n+1,0}^1 t_{n+1,b}^0 t_{n+1,0}^1 t_{n+1,b}^0 \quad (1.4)$$

$$t_{i,n+1}^k = t_{i,1}^k t_{i,n+1}^1 t_{i,1}^k t_{i,n+1}^1 \quad (1.5)$$

This shows that we indeed can generate all Toffoli generators involving the $n + 1^{\text{st}}$ bit. Hence $\langle T'_{n+1} \rangle$ generates all Toffoli generators $t_{i,j}^k$ and is thus the Toffoli group T_n . □

1.1.4 Infinite Toffoli group

The natural embedding of the Toffoli groups $T_n \hookrightarrow T_{n+1}$ forms a directed system. Let T_∞ be that direct limit; $T_\infty = \varinjlim T_n$. A group is locally finite if every finite collection of elements generates a finite subgroup. Any group which is the direct

limit of finite groups is locally finite. Since T_n is simple when $n > 3$ we conclude that T_∞ is a simple locally finite simple group of alternating type.

Locally finite simple groups have been stratified into 5 distinct families:

- Finite simple groups (Completely classified)
- Finite dimensional linear groups: these have a faithful representation as linear transformations of a finite dimensional vector space over a commutative field. (Completely classified)
- Finitary groups: these have a faithful representation as linear transformations of a vector space over a commutative field, such that every element differs from the identity by a transformation of finite rank. (Completely classified)
- Groups of p -type (or 1-type): every Kegel cover for the group has a subcover where each of the simple factors is a Lie type group of characteristic p (respectively an alternating group).
- Groups of ∞ -type: For any sequence of finite simple groups such that every finite group embeds into one of the terms of the sequence, there is a Kegel cover whose simple factors are among the terms of the sequence.

Here, a Kegel cover is a sequence $\{(H_n, M_n)\}$ where H_n is finite, H_n/M_n is simple, and $H_{n+1} \cap M_n = \{1\}$ for every n . The simple factors of a Kegel cover is the set of factors H_n/M_n . We will make use of this technical concept in a rather simple way, with $M_n = \{1\}$ and H_n simple.

Lemma 1.1.8. *If x is an element of order 3 in $G = T_\infty$ then $|O_3(C_G(x))| = \infty$. If X is infinite and x is an element of order 3 in $G = \text{Alt}(X)$ then $|O_3(C_G(x))| < \infty$.*

Proof. Here is a common setup to show both statements. For x an element of order 3, we have that $x = x_1x_2 \cdots x_s$ a product of 3-cycles. Let Y be the set of points it moves. Let E be the elementary abelian group generated by $\{x_1, x_2, \dots, x_s\}$. Centralizers of elements in the symmetric group over a set X are well known. The centralizer for x is $(E \rtimes B) \times \text{Sym}(X - Y)$, where B is the symmetric group of degree s permutes the s 3-cycles of x . Restricting this centralizer within $\text{Alt}(X)$, one gets the index 2 subgroup of alternating elements.

First we consider the case of $G = \text{Alt}(X)$. The element x has finite support and thus E is finite, Y is finite, and $X - Y$ is infinite. We have that $C_G(x) \subset (E \rtimes B) \times \text{Sym}(X - Y)$. The 3-core of $\text{Sym}(X - Y)$ is trivial, as an intersection with $\text{Alt}(X - Y)$ would be a normal subgroup to it. Thus the 3-core of the centralizer is contained within $E \rtimes B$, which is finite.

Let Ω_m be the elements moved by Toffoli group T_m . The element x is in T_m for some m , composed of s 3-cycles. By the embedding, x is the product of $2s$ 3-cycles in T_{m+k} . In general x is the product of $2^k s$ 3-cycles in T_{m+k} and moves $2^k 3s$ points Y_{m+k} . $O_3(C_{T_m}(x))$ embeds diagonally within $O_3(C_{T_{m+k}}(x))$, and thus $O_3(C_{T_\infty}(x)) = \bigcup_{k=0}^{\infty} O_3(C_{T_{m+k}}(x))$. Let E_{m+k} be the elementary abelian group generated by the 3-cycles of x in its embedding in T_{m+k} . As $E_{m+k} \subset O_3(C_{T_{m+k}}(x))$ and the size of E_{m+k} is unbounded as k increases, $O_3(C_{T_\infty}(x))$ has infinite order. \square

Finally, we introduce terminology required for the final section of the following

proof from [4]. Let H be a fixed group acting on a set Ω ($|\Omega| \geq 7$) as $\text{Alt}(\Omega)$. Let Λ be any set on which H acts, and Σ is an orbit of H in Λ . Σ is called Ω -essential if $C_H(\Sigma) \subseteq C_H(\Omega)$. Λ is called Ω -block-diagonal if every Σ -essential orbit Σ is isomorphic to Ω as a set acted upon by H .

Theorem 1.1.9. *T_∞ is a simple locally finite group of 1-type.*

Proof. Any finite group has a linear representation, and any linear group has a finitary representation. Now assume that T_∞ is finitary. By Theorem 5.2 in [6] there would be an infinite set X such that $T_\infty = \text{Alt}(X)$. However, by Lemma 1.1.8, one sees that they are distinctly different groups. Thus T_∞ is not finitary, linear, or finite.

For each n let Ω_n be the set of $2^n - n - 1$ binary strings of length n upon which T_n acts. T_∞ is of alternating type as every finite subgroup is naturally a subgroup of one of the finite groups T_n , which acts faithfully on Ω_n . Consider $H = T_5$ as a subgroup for any T_n with $n \geq 6$. There are 2^{n-5} orbits in Ω_n by H , each determined by the content of the upper $n - 5$ bits which are fixed by H . Ignoring those bits one sees that each orbit is isomorphic to Ω_5 as an H -set. Also $C_H(\Sigma) = C_H(\Omega_5) = \{1\}$ for each orbit Σ and thus each Ω_n is Ω_5 -block-diagonal. Using that $\{(T_n, 1)\}$ is a Kegel cover for T_∞ and Theorems 4.2 and 1.4 from [4], the group T_∞ is of 1-type. \square

1.2 Quantum Computation

Quantum computing originates with Quantum Physics. Physicist Richard Feynman wondered if quantum interactions could be used as a computing device, and whether it was different than classical Turing machines. Later David Deutsch created

the first algorithm which specifically made use of quantum effects. Finally, when Peter Shor found an extremely efficient algorithm to factor integers, many more researchers became interested and the field became quite popular.

Is there a physical limitation to computation? One of the things proved by Deutsch was that any computation which can be done by a classical machine could also be done with quantum computations. It appears that quantum computing is more powerful, and that many classically hard problems are easy in the new framework. For instance, there are more efficient factoring algorithms (Shor's Algorithm) and searching algorithms (Grover's Algorithm). Classical and quantum computing may be equally powerful, but no one has yet found evidence to support this. There is interest in seeing how efficiently quantum computing can be modeled in a classical setting.

The perceived additional power from quantum computing comes from acting on entangled particles in superposition. Upon observation, the quantum waveform collapses and the superposition destroyed so that a unique state is seen in the particles. The ability to work on more data than seems to be there (until observation) is a unique property that researchers wished to exploit.

However, in a paper by Albert Einstein, Boris Podolski, and Nathan Rosen (their initials lead the paper to be called the "EPR paper") the authors could not imagine that an unobserved particle did not possess physical properties which existed independent of observation. They also presumed that there must be some causality within the particle interactions which just was not apparent. They claimed that knowing physical properties existing at this level would allow someone to predict, with certainty, the outcome a state would have before it was measured. A simple probabilistic

experiment was later devised where the expected values of basic properties (taking on values of ± 1) would not exceed a certain bound if physical expectations of quantum mechanics held true. This is known as Bell's Inequality. This was experimentally shown to not hold for quantum mechanics.

Quantum interactions are modeled by unitary matrices acting on a complex projective space. The basic building block analog to the bit in quantum computing is the q-bit. Each q-bit is modeled in PC^2 , but realized in \mathbb{C}^2 by normalizing to length 1. In Dirac notation, basis vectors for \mathbb{C}^2 are given as $|0\rangle$ and $|1\rangle$. The q-bit $\alpha|0\rangle + \beta|1\rangle$, with $|\alpha|^2 + |\beta|^2 = 1$ is thought of as $|0\rangle$ with probability $|\alpha|^2$ and $|1\rangle$ with probability $|\beta|^2$. This corresponds to the superposition of a quantum state until it is observed. A q-bit and its negative are the same projectively, and their probabilistic states are identical.

Further q-bits are modeled in a tensor product of these complex spaces. A quantum string with 2 q-bits is modeled over $\mathbb{C}^2 \otimes \mathbb{C}^2$ for instance. For n q-bits, the space has complex dimension 2^n . For example, a string with 3 q-bits has basis vectors $|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle$. It is apparent that unitary matrices preserve the norm 1 condition. Also, this action is meant to represent quantum entanglement. Under a basis of $\{e_i\}$, a quantum entanglement of the possible states is $\sum \alpha_i e_i$ where $\sum |\alpha_i|^2 = 1$.

The power of quantum computing comes from this entanglement. A quantum computer can act on all 2^n basis vectors simultaneously, while a classical computer would need to handle each case separately. Entanglement also allows for intermediate combinations which only increases its usefulness. While there is no known limit to

how many q-bits natural processes can act on, the most powerful quantum computer constructed can operate on 7 (with its 128 combinations) [1]. The only issue is that results are found probabilistically. An algorithm must be run multiple times to ensure that the result is correct with a high degree of probability.

For instance, one might construct an algorithm which iterated $x_{n+1} = 2 * x_n^2$ for the integers modulo 4 using two q-bits (with $|11\rangle = 3$, etc.). If the machine was initialized with all states having equal likelihood, and the computation was halted and read after one step, then the machine would return $|00\rangle$ and $|01\rangle$ each with 1/2 likelihood. If read after more than one step, it would always return $|00\rangle$. Note that reading the state of a quantum machine destroys the entanglement and returns a specific binary string.

Researchers have been able to construct quantum circuits which perform operations on q-bits. The most basic of these objects are called universal quantum gates, as all quantum computations can be done by them. One interesting aspect to these gates is that they are reversible; there exists another gate (or series of gates) which can take the output back to the original input. Reversibility also exists in the quantum computing model, as a unitary matrix is invertible, and that inverse is also unitary. In fact, reversible computing is finding its way into modern computer CPUs, as destroying information takes more energy and causes more heat than propagating an unused result.

1.2.1 Classical Gates

Classical computation is handled by the classical gates: CNot (controlled not), Fredkin (controlled swap), and Toffoli (controlled-controlled not). These have been constructed for quantum computers, so that all computations which can be done classically may also be performed quantumly. The purely quantum gates which have been constructed are the Pauli, Hadamard, and Phase gates. We have seen the Toffoli groups (which contain all Fredkin and Toffoli gates).


Definition 4. *The (complex) Clifford Group is generated by the (complex) Pauli, Hadamard, Phase, and CNot gates. The real Clifford Group is generated by the real Pauli, Hadamard, and CNot gates.*

These are the complex/real groups which are generated with the discovered quantum gates, and including the CNot gate. Both of these groups are finite, and they have orders $2^{n^2+2n+3} \prod_{j=1}^n 4^{j-1}$ and $2^{n^2+n+2}(2^n - 1) \prod_{i=1}^{n-1} (2^{2i} - 1)$ respectively when acting on n q-bits [3]. Our interest is in the amalgam between the real Clifford group and the Toffoli group on a fixed number of q-bits.


1.2.2 Quantum Gates

A gate of fundamental importance is the Hadamard gate. It puts a single q-bit into superposition. If a q-bit has been read, then it has collapsed to either $|0\rangle$ or $|1\rangle$. If such a q-bit is passed through a Hadamard gate, then both possibilities become equally likely if a read is then performed. In unitary matrix form, the non-projective

Hadamard gate is:

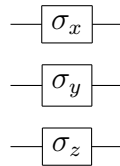
$$h := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$


The Phase gate sends $|1\rangle$ to $i|1\rangle$ and fixes $|0\rangle$.

$$ph := \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$


The Pauli gates are spin operators discovered by Wolfgang Pauli. They can be represented by the following matrices:

$$\sigma_x := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_y := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$



The Pauli matrices satisfy $\sigma_x^2 = \sigma_y^2 = \sigma_z^2 = I_{2 \times 2}$, and the determinant of each is -1 and the trace of each is 0 . These can be generated by the previous gates by $\sigma_z = ph^2$, $\sigma_x = h\sigma_z h$, and $\sigma_y = i\sigma_x\sigma_z$. For the last relation, σ_y acts the same as $\sigma_x\sigma_z$ projectively, the imaginary inclusion is there for the non-projective gate to be an involution. It is interesting to note that the Lie Algebra $\mathfrak{su}(2)$ is generated by

$i\sigma_x, i\sigma_y, i\sigma_z$.

Definition 5. *The complex Pauli group is generated by σ_x , σ_y and σ_z while the real Pauli group is generated only by σ_x and σ_z .*

Lemma 1.2.1. *Projectively the Pauli gates acting on n q-bits is an elementary abelian 2-group of order 4^n . The complex Pauli group is a class 2 nilpotent group of order 4^{n+1} with center $\{I, -iI, -I, -iI\}$ and derived subgroup $\{I, -I\}$. The real Pauli group is an “+”-type extraspecial group of order 2^{2n+1} .*

Proof. Consider the generators of the group; $3n$ gates where for each q-bit one has $\{\sigma_x, \sigma_y, \sigma_z\}$. If one selects generators for different q-bits, then they commute. Thus we need only focus on each individual q-bit, and here use the 2×2 matrix representation. One can check that the commutators satisfy $[\sigma_x, \sigma_y] = (\sigma_x \sigma_y)^2 = -I = [\sigma_y, \sigma_z] = [\sigma_z, \sigma_x]$. Projectively, $-I = I$ and thus all of the generators on a single bit commute in this case and generate a group of order 4. Hence the projective Pauli group on n q-bits is elementary abelian of order 4^n .

One can check that only diagonal matrices commute with σ_z , and to further commute with σ_x restricts attention only to multiples of the identity. Lifting a 2×2 multiple of the identity on one q-bit to a $2^n \times 2^n$ matrix acting on n q-bits gives us that same multiple of the respective identity matrix. The center of the non-projective Pauli group can thus only be multiples of the identity. Since $\sigma_y = i\sigma_x \sigma_z$, then $iI = \sigma_x \sigma_z \sigma_y$ is an element of the single q-bit group. Thus the center of the n q-bit Pauli group is $\{I, iI, -I, -iI\}$. The group modulo its center is the projective Pauli group, and thus the order of the non-projective group is 4^{n+1} . As elements are either purely real or

purely imaginary, commutators of elements have an even number of purely imaginary components, which multiply to a real number. Hence the derived subgroup is $\{I, -I\}$.

The real Pauli group is generated by σ_x and σ_z gates. As before, the projective real Pauli group on n q-bits is elementary abelian of order 4^n . The center, consisting of multiples of the identity, must be $\{I, -I\}$. The commutator subgroup is also $\{I, -I\}$. Thus the real Pauli group is an extraspecial group of order 2^{2n+1} . The elementary abelian subgroup generated by $-I$ and the n σ_z gates has order 2^{n+1} and thus the extraspecial group is of “+”-type. \square

The classical gates CNot and Toffoli can also be represented in the quantum setting and each has a related gate for wire diagrams. CNot is a 2 q-bit gate similar to the 3 q-bit gate Toffoli. To perform a not on the second bit if and only if the first is set reduces to permuting $|10\rangle$ and $|11\rangle$.

$$c_1^0 := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$



This wire diagram shows that the upper q-bit is the control and the lower bit is the target. The Toffoli gate is drawn similarly, since it has two control q-bits acting on

one target q-bit.



1.2.3 Another Generation of the Clifford Group

The Pauli group is a normal subgroup of the Clifford group (and in fact it is the 2-core of the Clifford group) [5] but we will attempt the opposite in this section - show that the normalizer of the real Pauli group in its natural linear group is the real Clifford group. Henceforth Pauli and Clifford will mean the real version of those groups. Along the way, the intersection of the Clifford group and all monomial matrices will be found. This intersection is important for identifying the amalgam between the Clifford Group and the Toffoli group.

For a given linear group, there is a natural vector space V upon which it acts. We define a frame for V to be a collection of 1-spaces $F = \{\langle v_1 \rangle, \langle v_2 \rangle, \dots, \langle v_n \rangle\}$ in V such that $\{v_1, v_2, \dots, v_n\}$ is a basis for V . G is said to fix the frame F if G permutes these 1-spaces. It can be the case that for a given linear group there are many frames which it fixes.

One thing to notice is that if G fixes a frame F and x is in the normalizer of G in $GL(V)$, then G fixes $x \cdot F$. The converse is not true. This is because if $G^x \cdot F = F$, then $x^{-1}Gx \cdot F = F$. Thus $G \cdot (x \cdot F) = x \cdot F$ and G fixes this potentially new frame. We will show that for the Pauli group, the converse is true.

For this section, we let G be the group generated by the Pauli-x and Pauli-z operators on n q-bits (σ_x and σ_z). Recall that G is an extraspecial group of order

2^{2n+1} and is of “+”-type. The natural vector space acted upon by G is \mathbb{R}^{2^n} .

Lemma 1.2.2. *An abelian group H acting transitively on a set X is fixed-point free.*

Proof. If X contains one or two points, the conclusion is clear. If X contains three or more points, we argue by contradiction. Suppose that H is not fixed-point free. Then there are elements x, y, z in X and τ in H such that $\tau \cdot x = x$ and $\tau \cdot y = z$. H transitive implies that there is an element σ in H where $\sigma \cdot x = y$. $\tau\sigma \cdot x = \tau \cdot y = z$. $\sigma\tau \cdot x = \sigma \cdot x = y$. H abelian implies that $z = y$, which is a contradiction.

□

A generic elementary abelian group of order 2^n shall be denoted E_{2^n} .

Theorem 1.2.3. *Suppose that F is a frame for G in \mathbb{R}^{2^n} . Then there is a normal elementary abelian subgroup of G which is the stabilizer of each 1-space of F . Furthermore, the frame is the collection of eigenspaces for this subgroup.*

Proof. We first invoke character theory to show that G acts irreducibly on \mathbb{C}^{2^n} and thus \mathbb{R}^{2^n} . Let χ be the character of G on \mathbb{C}^{2^n} . $\chi(I) = 2^n$ and $\chi(-I) = -2^n$. The pure Pauli-z elements and their negatives are diagonal matrices with an equal number of 1 and -1 entries and thus have trace 0. The rest of the elements are monomial with diagonal entries all 0. Hence for all $g \in G$ which are not $\pm I$, we have $\chi(g) = 0$. The inner product of χ with itself is $[\chi, \chi] = 2^{-(2n+1)}(2^{2n} + 2^{2n}) = 1$, showing that χ is an irreducible character and thus \mathbb{R}^{2^n} is an irreducible module.

G permutes the 1-spaces of F and its center, $\{\pm I\}$, fixes them. Hence $G/Z(G) \cong E_{2^{2n}}$ permutes the 1-spaces. This permutation is transitive as G is irreducible on

\mathbb{R}^{2^n} . By Lemma 1.2.2, this transitive abelian action is fixed-point free. Let K be the kernel of the permutation action. This is also a point stabilizer by the same Lemma, so $|G/K| = |F| = 2^n$ and $G/K \cong E_{2^n}$.

Now, K has order 2^{n+1} and fixes the 1-spaces of F . Thus K is abelian since it acts on \mathbb{R}^{2^n} as a direct sum of one dimensional modules. If K were to have an order 4 element k , then for some $\langle v \rangle \in F$ we would get $k \cdot v = iv$ or $-iv$ which cannot happen over the reals. Thus K is elementary abelian of order 2^{n+1} . \square

Theorem 1.2.4. *Suppose K is an elementary abelian subgroup of G of order 2^{n+1} which includes the center of G . Then K has 2^n distinct orthogonal eigenspaces in \mathbb{R}^{2^n} . Furthermore, the full group permutes these eigenspaces, so that they are a frame.*

Proof. Let \hat{K} be any subgroup of K missing $-I$ of order 2^n . For instance, thinking of K as a vector space over the field of 2 elements, one can generate such a codimension 2 subspace. Again, the trace of the identity is 2^n and all other elements of \hat{K} have trace 0. Hence \mathbb{R}^{2^n} decomposes into the direct sum of 2^n distinct 1-dimensional modules for \hat{K} . These modules are then eigenspaces for K after including $-I$.

For a given eigenspace $\langle v \rangle$, now let \hat{K} be the kernel in K of the action on $\{v, -v\}$. As $-I \in K$ we see that \hat{K} has index 2 and the preceding module decomposition holds. Thus, if one picks another eigenspace $\langle w \rangle$, then there is a $k \in \hat{K}$ such that $k \cdot w = -w$. Now, k is an orthogonal matrix, so its action has no effect on the standard inner product: $\langle v, w \rangle = \langle k \cdot v, k \cdot w \rangle = \langle v, -w \rangle$. Adding $\langle v, w \rangle$ to both sides shows that $2\langle v, w \rangle = \langle 2v, 0 \rangle = 0$, giving orthogonality. Since the choice of $\langle v \rangle$ and $\langle w \rangle$ among eigenspaces was arbitrary, the eigenspaces are orthogonal.

Finally we notice that K is normal in G via the correspondence theorem as $K/Z(G)$ is normal in $G/Z(G)$. So, if $x \in G$ and we let F be the set of eigenspaces, then $K^x \cdot F = F$. Thus $K \cdot (x \cdot F) = x \cdot F$ and so $x \cdot F$ is a collection of eigenspaces fixed by K . Thus $F = x \cdot F$ as there is only one collection of eigenspaces for K , and F is a frame for G . \square

Theorem 1.2.5. $x \in N_{\text{GL}(\mathbb{R}^{2^n})}(G)$ if and only if $x \in \text{O}_{2^n}(\mathbb{R})$ permutes the frames of the Pauli group G .

Proof. Since the frames are all orthogonal, we immediately have that the normalizer of the Pauli group must be an orthogonal group. When $x \in N(G)$, x always permutes the frames of G . The converse will also be true in this case.

If x permutes the frames of G then G^x has the same frames as G . Let F be a frame of G . By Theorem 1.2.3, G has an elementary abelian 2-subgroup K of order 2^{n+1} which acts \mathbb{R}^{2^n} as a direct sum of the one dimensional modules forming the frame. Let \hat{K} be a subgroup of K of order 2^n missing $-I$. \mathbb{R}^{2^n} decomposes into 2^n distinct 1-dimensional modules over \hat{K} . Then each element of \hat{K} is a diagonal matrix in a basis extracted from the frame. Since \hat{K} is abelian it is isomorphic to its linear characters as a group. Thus the elements of \hat{K} are determined collectively - their entries are completely determined via the characters.

Thus a given frame F determines exactly the matrices forming K . The same is true of G^x , and so K is the subgroup of G^x corresponding to the frame F . G^x must then contain the elementary abelian 2-subgroups generated by the Pauli-x elements with $-I$ and the Pauli-z elements with $-I$. These generate G and thus $G^x = G$. \square

Proposition 1.2.6. *The number of maximal elementary abelian subgroups in an extraspecial 2-group G of “+”-type of order 2^{2n+1} is $2 \prod_{k=1}^{n-1} (2^k + 1)$.*

Proof. There is a well defined symplectic form on the elementary abelian 2-group $E = G/Z(G)$, of dimension $2n$. For $x, y \in E$ define $(x, y) = [xZ(G), yZ(G)]$, which takes values in $Z(G)$. Call these values 0 and 1, for the identity and non-identity elements respectively. Notice that there is a 1-1 correspondence between the abelian groups of G of order 2^{m+1} which contain the identity and totally isotropic subspaces of E of dimension m , since $(x, y) = 0$ is equivalent to x and y commuting. The form is non-degenerate (as the center is order 2) and maximal totally isotropic subspaces are of dimension n , so that the maximal abelian subgroups have order 2^{n+1} and include the center. We count them now.

The symplectic group $\text{Sp}(E)$ is transitive on maximal totally isotropic subspaces. Let E have symplectic basis $\{e_1, e_2, \dots, e_n, f_1, f_2, \dots, f_n\}$, where $(e_i, f_i) = (f_i, e_i) = 1$ (recall this is over the field of two elements) and all others are 0. If $\{\tilde{e}_1, \tilde{e}_2, \dots, \tilde{e}_n\}$ is a basis for a maximal totally isotropic subspace, expand this to a hyperbolic basis by selecting an \tilde{f}_j perpendicular to the subspace and previous \tilde{f}_i such that $\{\tilde{e}_j, \tilde{f}_j\}$ is a hyperbolic pair. By definition, $\text{Sp}(E)$ has a transformation L with $L(e_i) = \tilde{e}_i$ and $L(f_i) = \tilde{f}_i$. The stabilizer of the span of $\{e_1, e_2, \dots, e_n\}$ in $\text{Sp}(E)$ is upper block triangular. Verify that it has the form

$$\left\{ \begin{pmatrix} A & XA \\ 0 & (A^{-1})^T \end{pmatrix} \mid A \in \text{GL}_n(\mathbb{F}_2), \quad X + X^T = 0 \right\}$$

This has order $2^{n^2} \prod_{k=1}^n (2^k - 1)$. The order of $\text{Sp}(E) = \text{Sp}_{2n}(\mathbb{F}_2)$ is known to be $2^{n^2} \prod_{k=1}^n (4^k - 1)$. Thus the number of maximal totally isotropic subspaces is $\prod_{k=1}^n (2^k + 1)$.

Since G is of “+”-type, there are two kinds of maximal abelian subgroups. Type (A) will be the elementary abelian groups of order 2^{n+1} , and type (B) will be the direct product of a cyclic group of order 4 with an elementary abelian group (not containing the center) of order 2^{n-1} . We next create a simple geometry by saying that a type A and type B subgroup are incident if they intersect in an elementary abelian group of order 2^n . Let F be any elementary abelian subgroup of order 2^n and \tilde{F} be a maximal subgroup missing the central element of order two. Let W be $(F/Z(G))^\perp$ in the symplectic space, so the dimension of W is the codimension of $F/Z(G)$ which is $n + 1$. In G , W corresponds to $\tilde{F} \times D$, where D is a dihedral group of order 8. Any subgroup of $\tilde{F} \times D$ of type A or B is a direct product of \tilde{F} and a subgroup of order 4 in D . D has one cyclic subgroup of order 4 and two Klein four groups containing the center. Thus $\tilde{F} \times D$ contains one type B and two type A's, and F is only contained in exactly these.

A type B subgroup contains one elementary abelian subgroup of order 2^n (its the subgroup of elements not of order 4), and thus is incident to two type A's. Thinking of a type A subgroup as a vector space of dimension $n + 1$ over \mathbb{F}_2 , each has $2^n - 1$ subspaces of dimension n which include the 1 dimensional subspace $Z(G)$. Thus each type A subgroup is incident to $2^n - 1$ type B subgroups. This means that for every type A, there are $\frac{1}{2}(2^n - 1)$ type B subgroups. Or, for every type A, there are $\frac{1}{2}(2^n + 1)$ of either type. Dividing this value into the total number of maximal abelian

subgroups gives the number of which are type A subgroups, and thus the desired result. \square

As an immediate corollary, we have that the number of frames for the Pauli group in dimension 2^n is $2 \prod_{k=1}^{n-1} (2^k + 1)$. If the normalizer were to be transitive on the frames, we would only need to find the order of a frame stabilizer (say the standard frame) to find the order of the Clifford Group.

<i>Dimension</i>	<i>Frames</i>
2^1	$\langle e_0 \rangle, \langle e_1 \rangle$ $\langle e_0 + e_1 \rangle, \langle e_0 - e_1 \rangle$
2^2	$\langle e_{00} \rangle, \langle e_{01} \rangle, \langle e_{10} \rangle, \langle e_{11} \rangle$ $\langle e_{00} + e_{11} \rangle, \langle e_{00} - e_{11} \rangle, \langle e_{01} + e_{10} \rangle, \langle e_{01} - e_{10} \rangle$ $\langle e_{00} + e_{01} \rangle, \langle e_{00} - e_{01} \rangle, \langle e_{11} + e_{10} \rangle, \langle e_{11} - e_{10} \rangle$ $\langle e_{00} + e_{10} \rangle, \langle e_{00} - e_{10} \rangle, \langle e_{11} + e_{01} \rangle, \langle e_{11} - e_{01} \rangle$ $\langle e_{00} + e_{01} + e_{10} + e_{11} \rangle, \langle e_{00} - e_{01} + e_{10} - e_{11} \rangle,$ $\langle e_{00} + e_{01} - e_{10} - e_{11} \rangle, \langle e_{00} - e_{01} - e_{10} + e_{11} \rangle$ $\langle -e_{00} + e_{01} + e_{10} + e_{11} \rangle, \langle e_{00} - e_{01} + e_{10} + e_{11} \rangle,$ $\langle e_{00} + e_{01} - e_{10} + e_{11} \rangle, \langle e_{00} + e_{01} + e_{10} - e_{11} \rangle$

Table 1.1: The Frames for the smallest Pauli Groups

Let us now focus on the stabilizer in $N(G)$ of the standard frame. Any element which fixes the standard basis is a monomial group. The monomial matrices which are orthogonal are signed permutation groups. To get an idea of the intersection of the Toffoli and Clifford groups (which is useful for studying the coset geometry) we will look at a collection of unsigned permutation matrices which normalize the Pauli group.

The Pauli-x gates act like NOT gates and Pauli-z gates act as NEG(ation). On the k^{th} bit these will be denoted X_k and Z_k respectively. Recall that the CNot operator with bit i as control and j as target is c_j^i , and that it is its own inverse. Verify that

conjugation of the basic Pauli gates by CNot gates give the following:

$$c_j^i X_k c_j^i = \begin{cases} X_k & k \neq i, j \\ X_i X_j & k = i \\ X_j & k = j \end{cases} \quad c_j^i Z_k c_j^i = \begin{cases} Z_k & k \neq i, j \\ Z_i & k = i \\ -Z_i Z_j & k = j \end{cases}$$

This demonstrates that the collection of CNot gates are in the normalizer. Let us attempt to get a handle on how this part of the normalizer acts on the Pauli group.

The center of the Pauli group is $\{-I, I\}$, so the normalizer of the group would automatically normalize these elements. Thus we will focus on the head of the extraspecial group, which is just an extraspecial 2-group. Let V_X and V_Z be the vector spaces over the field of two elements defined by the Pauli-x and Pauli-z gates respectively, quotienting out $\{-I, I\}$. Call the quotients by the center \bar{X}_k and \bar{Z}_k on bit k . The CNot gates act on these vector spaces, by conjugation on the generators, and are thus elements of $\text{GL}(V_X)$ and $\text{GL}(V_Z)$. Consider the commutator $[c, v] = c \cdot v - v$ of a CNot operator on each vector space. We have $[c_j^i, V_X] = \text{span}_{\mathbb{F}_2} \langle \bar{X}_j \rangle$, and $[c_j^i, V_Z] = \text{span}_{\mathbb{F}_2} \langle \bar{Z}_i \rangle$.

In both cases these are transvections. Thus the full special linear groups are achieved on V_X and V_Z . Hence $\text{GL}(V_X)$ and $\text{GL}(V_Z)$ as both vector spaces are over \mathbb{F}_2 . How does the unsigned permutation group portion of the normalizer act on $V_X \oplus V_Z$? We've seen before in this section that this vector space comes with a symplectic/orthogonal form (since the characteristic of the field is 2). Future effort could be in finding Seigel elements here, what portion of the Toffoli group normalizes

the Pauli group, and the remainder of the normalizer.

Since the Clifford Group normalizes the Pauli group, the Hadamard gates must also act on the frames. It appears that the Hadamard and CNot gates are transitive over all frames, but this has not been proven. All frames for each Pauli group can be determined quickly by starting with the standard frame and applying the Hadamard and CNot gates to various bits. The interaction of the two groups generated by these gates also would be interesting to study.

Chapter 2

Geometry

A geometry is a generalization of a graph. A graph has a vertex set V and an edge set $E \subseteq V \times V$ where $(x, y) \in E$ means that the points x and y are connected by an edge. For a geometry, we introduce a finite set I and a function $\tau : V \rightarrow I$ which we say colors the vertices and is called the type function. We demand that τ is onto I , and $|I|$ is called the rank of the geometry. The set (V, E, I, τ) is a geometry if (V, E) is a graph and whenever (x, y) is an edge then $\tau(x) \neq \tau(y)$.

A flag in a geometry is a set of vertices T which form a clique (all are incident). Necessarily the type or color of each vertex must be different. The rank of a flag is the number of elements in T . A flag is said to be maximal if it achieves the highest rank attainable in a given geometry. A flag has full rank if $\tau(T) = I$.

An example of a geometry is a vector space V . Here, the vertices of the graph are the subspaces and τ maps a subspace to its dimension. So $I = \{0, 1, \dots, \dim(V)\}$. Two vertices are incident in the graph if they represent different subspaces and one is properly contained in the other. A flag in this geometry is a set of subspaces which

form a chain under proper containment. Full rank flags exist in this geometry; they have the 0-space contained in a 1-space contained ... contained in the full vector space.

A category is a collection of objects and maps between them called morphisms which preserve various properties of the objects through the maps. Morphisms must satisfy the following: the composition of two morphisms (with the range object of one being the domain of the other) must be a morphism, and that the identity map on an object is a morphism. The collection of all morphisms from an object to itself are the endomorphisms of that object and the endomorphisms which are isomorphisms are called automorphisms. The collection of all automorphisms of an object forms a group under composition.

Group actions on sets can be reformulated in this language. The category of sets consists of objects which are sets and morphisms are functions between sets. The automorphism group of an object in this category would be the full symmetric group on that object (set). A group which acts on a set can be mapped homomorphically into the automorphism group of the set. For a graph, we demand that morphisms map non-incident vertices to non-incident vertices and that incident vertices will be mapped to incident vertices or the same vertex. Furthermore, for a geometry, we want that the color/type of a vertex is preserved under any morphism. Necessarily for any two geometries to have morphisms between them requires that they have the same index set I . If a group acts on a geometry, then it has a homomorphic image into the automorphism group of that object in the category of geometries.

A group which acts on a geometry is flag transitive if for any two flags T and T'

with $\tau(T) = \tau(T')$ there is an element of the group which takes each element of T to an element of T' .

In our vector space example, $\text{GL}(V)$ is the automorphism group of the geometry and it is flag transitive. For a given flag T , find a basis of the smallest subspace and continue to expand that basis to one for increasingly larger subspaces, and then expanding it to the full space as necessary. For another flag T' with $\tau(T) = \tau(T')$, one can construct a basis in the same way. One can see that $\text{GL}(V)$ has an element which takes one basis to the other, and hence maps one flag to another.

Another important example of a geometry is one associated with groups. For a fixed group G and a finite number of distinct subgroups H_1, H_2, \dots, H_n set the vertices of the graph to be the cosets of these subgroups. The type of the vertex is the index of the subgroup which it is based on. Two vertices are incident if their corresponding cosets intersect (but are not equal). Unfortunately in this setting, the highly desirable property of flag transitivity is only guaranteed for geometries of rank 2. For if $gH_1 \cap kH_2 \neq \emptyset$ then k^{-1} sends the cosets to $k^{-1}gH_1$ and H_2 . If h is in their intersection (which is not empty) then $1 \in hk^{-1}gH_1$ thus we must have the coset of the identity - the original subgroup. Thus $hk^{-1}g$ takes the original cosets to H_1 and H_2 (as H_2 is fixed by h).

2.1 Analysis of the Coset Geometry

The group generated by the Clifford Group and the Toffoli Group (on a given number of inputs) is generated by two of its finite subgroup, and the coset geometry

has infinite diameter. This means that quantum computations are unbounded - for any given computation there is another one which takes more steps. This result is true for any group generated by two finite subgroups, say A and B . There are at most $|A|$ cosets of B which intersect A non-trivially (and thus have distance 1 from A). There are at most $|A| |B|$ cosets of A which are distance 2 from A . In general, there are at most $|A|^{n+1} |B|^n$ cosets of B which are distance $2n + 1$ and at most $|A|^n |B|^n$ cosets of B which are distance $2n$ from A . Hence there are only a finite number of cosets within a fixed distance of one of the subgroups, and thus only a finite number of elements in their union as the subgroups are finite. Since the group is infinite, no finite distance in the coset graph will contain all of the groups elements.

The Toffoli group is self normalizing in the amalgam, as is the Clifford group. This affords us a nice relation between the coset geometry, and another geometry called the conjugate geometry. Let A be a subgroup of a group G , then $\{g_i N(A)\}$ are distinct cosets for $N(A)$ for some index set I and representatives g_i . Then we have that $\{A^g | g \in G\} = \{A^{g_i} | i \in I\}$. It must be that $A^{g_i} = A^{g_j}$ if and only if $g_i \in g_j N(A)$ which occurs if and only if $g_i = g_j$ as they are coset representatives. The action on the cosets of the normalizer of a subgroup directly corresponds to the action (by conjugation) on the conjugates of that subgroup. Now assume that we have two subgroups A and B , which are both self-normalizing. In coset geometry, two cosets are incident when they have non-trivial intersection. In conjugate geometry, A^h being incident to B^k corresponds to the existing an element g such that $A^g = A^h$ and $B^g = B^k$.

2.2 Tensor Products

Let V and W be vector spaces over a field k , with basis $\{v_i\}$ and $\{w_j\}$ respectively. Let U be the subgroup of the free abelian group $V \times W$ with $U = \{(v\alpha, w) - (v, \alpha w) | v \in V, w \in W, \alpha \in k\}$. The tensor product of these spaces V and W is a vector space $V \otimes W$ defined as the homomorphic image of $V \times W$ under U . It has as its basis $\{v_i \otimes w_j\}$. The tensor product of two linear maps f and g is the bilinear map $f \otimes g$ where, on the basis, $f \otimes g(v_i \otimes w_j) = f(v_i) \otimes g(w_j)$.

If one were to apply a gate which works on n q-bits on that many of an $m > n$ q-binary string, then the 2^m by 2^m matrix representing this gate on a larger system is found by the Kronecker product of a permutation matrix with the matrix for the gate over the n q-bit system. The Kronecker Product of two matrices is a matrix over the tensor product of the original bases. It is the matrix of the tensor product of the two linear transformations represented by the original matrices. The values are computed as $A \otimes B(e \otimes f) = A(e) \otimes B(f)$. For example, the Kronecker product between the 2x2 identity and 2x2 Hadamard is:

$$I_{2 \times 2} \otimes h = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

One focus of ours will be in Kronecker products of permutation matrices and Hadamard gates.

Chapter 3

Main Theorem

The group of real quantum operators is known to be an orthogonal group (and unitary in the complex case). Here, a larger orthogonal group will be found containing it. The Clifford Group and Toffoli groups generate the group of quantum operators, where the Toffoli group is alternating on all length n binary strings of bit weight at least 2. Now consider the group which is generated by the Clifford Group and the full signed alternating group on all binary strings of length n . We will show that this group is $\text{SO}_{2N}(\mathbb{Z}[1/2]).\langle H \rangle$ and will consider ways to make use of this information in later chapters. Here the “.” means that the first group is a subgroup of the full group and the full group is generated by the subgroup and a lone Hadamard gate $H = h \otimes I \otimes I \otimes \cdots \otimes I$.

Definition 6. Let R be a ring, define $R\{\alpha\} = \cup_{n=0}^{\infty} R\alpha^n$, the multiplicative monoid generated by R and α . Note: if $\alpha \in R$ then $R\{1/\alpha\} = R[1/\alpha]$ is a ring.

Definition 7. P_{2N} is the set of signed $2N \times 2N$ permutation matrices.

Main Theorem. $\mathrm{SO}_{2N}(\mathbb{Z}[1/2]).\langle H \rangle = \langle H^\sigma \mid \sigma \in P_{2N} \rangle$

3.1 Proof of the Main Theorem

We will need the following definitions. For $z \in \mathbb{Z}\{1/\sqrt{2}\}$, we have that $z = y/2^{w/2}$, with $y \in \mathbb{Z}$. Define the weight of such an element to be w which is the minimal power of $2^{1/2}$ whose product with z is an integer. Call \bar{a} the integer part of a with respect to w when $\bar{a} = 2^{w/2}a$ is an integer. Define the weight of a matrix in $\mathrm{GL}_{2N}(\mathbb{Z}\{1/\sqrt{2}\})$ to be the maximum weight of its entries. This weight is also the minimal power of $2^{1/2}$ whose product with that matrix is an integer matrix. The weight of a row or column of this type of matrix is defined similarly.

The following, while trivial, is used a number of times and thus is presented here.

Lemma 3.1.1. *Let A, B be matrices in $M_{2N \times 2N}(\mathbb{Z}\{1/\sqrt{2}\}) \cap O_{2N}(\mathbb{R})$ with weights w_A, w_B respectively. Let w_{AB} be the weight of AB . Then $w_{AB} \leq w_A + w_B$. Moreover, $w_{AB} = w_A + w_B \pmod{2}$.*

Proof. $AB = 2^{(w_A + w_B)/2} X$ where X is an integer matrix. □

Consider a vector space of dimension $2N$ over $\mathbb{Z}\{1/\sqrt{2}\}$, with ordered the basis $(e_1, f_1, e_2, f_2, \dots, e_N, f_N)$. Set h to be the negative of the standard 2×2 Hadamard matrix, $h = -\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Define H on $(\mathbb{Z}\{1/\sqrt{2}\})^{2N}$ by the left action of h on the pair (e_i, f_i) . Equivalently, H is the Kronecker product $h \otimes I_N$, with I_N being the $N \times N$ identity matrix.

Let $S_{2N} = \{2^{-w/2}X | X \in M_{2N \times 2N}(\mathbb{Z}), X^T X = 2^w I_{2N}\}$. Notice that for $X \in S_{2N}$, the weights of each element of X have the same parity. In particular, the weight of each column has the same parity.

Lemma 3.1.2. $P_{2N} \subset \langle H^\sigma | \sigma \in P_{2N} \rangle$ for $2N \geq 4$.

Proof. Begin with the basis $\{e_1, e_2, \dots, e_{2N}\}$ and let A be a matrix in P_{2N} . We will select permutations $\{\sigma_1, \dots, \sigma_k\}$ such that $H^{\sigma_k} \dots H^{\sigma_1} A$ is the identity, and for $j < k$ $H^{\sigma_j} \dots H^{\sigma_1} A$ will have a block which is the identity. In this way, $A = H^{\sigma_1} \dots H^{\sigma_k}$, which demonstrates the desired result.

For $2N > 4$, there are four possibilities for the location and sign of the non-zero entry of the first column. If $A_{1,1} = 1$ (case 1), continue by induction on the $2N - 1 \times 2N - 1$ sub-block on indices 2 through $2N$. For the remaining three cases, let $\sigma_i(j) = \sigma_{i+1}(j)$ for $i > 2$. Suppose $A_{s,1} = -1$, with $s \neq 1$ (case 2). Let σ_1 and σ_2 be permutations with $\sigma_1(1) = \sigma_2(2) = 1$ and $\sigma_1(2) = \sigma_2(1) = s$. Then $A' = H^{\sigma_2} H^{\sigma_1} A$ is a matrix in P_{2N} and $A'_{1,1} = 1$, bringing us to the previous case.

If $A_{s,1} = 1$, with $s \neq 1$ (case 3), then there is a t with $A_{t,1} = 0$ since $2N > 4$. Let σ_3 and σ_4 be permutations with $\sigma_3(1) = \sigma_4(t) = s$ and $\sigma_4(2) = \sigma_3(1) = t$. Then $A' = H^{\sigma_4} H^{\sigma_3} A$ is a matrix in P_{2N} and $A'_{t,1} = -1$ and $t \neq 1$, which is case 2. Finally, suppose $A_{1,1} = 1$ (case 4). Let σ_5 and σ_6 be permutations with $\sigma_5(1) = \sigma_6(2) = 1$ and $\sigma_6(2) = \sigma_5(1) = s$, for some $s > 1$. Then $A' = H^{\sigma_6} H^{\sigma_5} A$ is a matrix in P_{2N} and $A'_{s,1} = -1$, bringing us to the previous case. Thus in all cases, we can find a series of permutations such that their conjugations with H leave a 1 in the $(1, 1)$ position, and continue inductively.

For $2N = 4$ we may assume that $A_{1,1} = 1$ by the methods above. Let $\sigma = (3\ 4)$ and note that projectively HH^σ acts as the permutation $(e_3\ e_4)$. For $\sigma_1 = (2\ 3)$ and $\sigma_2 = (2\ 3\ 4)$ note that H^{σ_1} and H^{σ_2} both pair row 1 with 3 and 2 with 4. Projectively $H^{\sigma_2}H^{\sigma_1}$ acts as the permutation $(e_2\ e_4)$. Thus the group generated by HH^σ and $H^{\sigma_2}H^{\sigma_1}$ acts projectively as the symmetric group on $\{e_2, e_3, e_4\}$. Hence there is an element H' in that group such that $A' = H'A$ is a diagonal matrix with $A'_{1,1} = 1$.

If A is a 4×4 diagonal matrix with $A_{1,1} = 1$, then either two or zero diagonal elements are -1 as the determinant is 1. The squares of the previous Hadamard products are diagonal: $(HH^\sigma)^2$ and $(H^{\sigma_2}H^{\sigma_1})^2$ have two 1 and two -1 entries. Either A is the identity, one of the two squares of Hadamard products, or their product. \square

The following theorem shows that the group of quantum operators, seen as an amalgam of the Clifford and Toffoli groups, is a subgroup of $\text{SO}_{2N}(\mathbb{Z}[1/2]).\langle H \rangle$. Note that signed permutations are not required in the following proof until the last step. If the above Lemma 3.1.2 could be shown to be true for defining P_{2N} to instead be only non-signed permutation matrices, then the result would be strengthened. Further note that the permutations used can be restricted to those which are even. The Toffoli Group is isomorphic to $\text{Alt}(2^{2N} - 2N - 1)$, which is nearly the full alternating group. This gives a feeling about how closely the group of quantum operators fits into its overgroup.

Main Theorem.

$$\langle H^\sigma | \sigma \in P_{2N} \rangle = \text{SO}_{2N}(\mathbb{Z}[1/2]).\langle H \rangle = M_{2N \times 2N}(\mathbb{Z})\{1/\sqrt{2}\} \cap \text{SO}_{2N}(\mathbb{R})$$

Proof. The containments from left-to-right are obvious, as $\det(H) = 1$ and H along with every permutation matrix is orthogonal. Given $X \in S_{2N}$, a (left) inverse shall be constructed from elements of the form H^σ where $\sigma \in P_{2N}$. We will induct on the dimension, $2N$.

Consider the first column of X as a vector, with entries a_1, a_2, \dots, a_{2N} . As X is orthogonal, $\sum_{i=1}^{2N} a_i^2 = 1$. If w is the weight of the column, we can consider the integer part of these entries with respect to w , and notice that $\sum_{i=1}^{2N} \bar{a}_i^2 = 2^w$. If the weight is 0, then it is necessarily the case that for a single j we have $a_j = \bar{a}_j = 1$ and all other a_i 's are 0.

Otherwise, when the column weight is positive, we have $0 = \sum_{i=1}^{2N} \bar{a}_i^2 = \sum_{i=1}^{2N} \bar{a}_i \pmod{2}$. Hence we have an even number of odd \bar{a}_i 's and similarly an even number of even elements. Choose any permutation $\sigma \in P_{2N}$ of the elements such that under the new ordering, when considered in our ordered basis $\{e_i, f_i\}$, each e_i and f_i have the same parity for all i . Now, $e_i \pm f_i$ is even, so $h(e_i, f_i) = (-(e_i + f_i)/\sqrt{2}, -(e_i - f_i)/\sqrt{2})$ has weight at most the weight of $\{e_i, f_i\}$ minus 1. Hence $H^\sigma X$ is an element of S_{2N} and it has a weight strictly less than w for its first column. This argument may be continued until the weight of the first column is 0.

With the first column having weight 0, we can focus our attention on the second column (in fact, one could consider the first two columns simultaneously). We wish

to pair these in such a way to get a 2×2 identity matrix. The entries of this column are b_1, b_2, \dots, b_{2N} . Suppose that $a_j = 1$, and the rest are 0. Note, by orthogonality, that $0 = \sum_{i=1}^{2N} a_i b_i = b_j$. Let w be the weight of the second column. For $w = 0$, then $b_k = 1$ for some $k \neq j$ with all others 0. If $w > 0$, then w is even as all columns have the same parity. Pick a permutation σ_1 that pairs the b_i in all even and all odd groups, just like above. Without loss, $\sigma_1(1) = j$ and let $k = \sigma_1(2)$. The second column of $H^{\sigma_1}X$ has entries c_1, c_2, \dots, c_{2N} . Now, pick a new permutation σ_2 , so that $\sigma_2(1) = \sigma_1(1)$ and $\sigma_2(2) = \sigma_1(2)$ and the remaining c_i are paired as above ($c_j = c_k \pmod{2}$ by orthogonality). $H^{\sigma_2}H^{\sigma_1}X$ preserves the first column of X , and decreases the weight of the second column. This occurs since H^{σ_1} and H^{σ_2} must both, in turn, reduce the weight, and the weight is odd (and thus positive) when H^{σ_2} is applied. This argument may be continued until the weight of the first two columns is 0.

Now, by considering the inner product of a row with itself, the j^{th} and k^{th} rows have one non-zero entry. Hence, under a permutation, we have a 2×2 identity block and a block of size $2(N-1) \times 2(N-1)$ in $S_{2(N-1)}$. The above argument can be repeated, using permutations which fix the already finished rows.

Now we are left with a signed permutation matrix. By the previous Lemma 3.1.2, this is in the group.

□

Note that replacing the full alternating set of matrix permutations with the actual Toffoli Group does not give the same result. However it should be the case that, if care is taken at each stage to select a permutation which is Toffoli, then the algorithm

should decompose quantum operators into a product of Clifford and Toffoli gates. Also note that each Pauli gate is contained in $SO_{2N}(\mathbb{Z}[1/2]).\langle H \rangle$, and thus Hadamards will be the only non-classical gate which will be represented in a decomposition. Finally, define the decomposition length of a matrix to be the minimal length it can be decomposed in products of the form H^σ .

Theorem 3.1.3. *Let A, B be elements of $SO_{2N}(\mathbb{Z}[1/2]).\langle H \rangle$. Define $d(A, B)$ to be either the weight or decomposition length of $A^{-1}B$. Then $d(\cdot, \cdot)$ is a metric on the coset space $SO_{2N}(\mathbb{Z}[1/2]).\langle H \rangle/P_{2N}$.*

Proof. We have that $d(A, B) \geq 0$ and if $d(A, B) = 0$ then $A^{-1}B \in P_{2N}$ so $AP_{2N} = BP_{2N}$. Note that $A^{-1} = A^T$, so A and A^{-1} have the same weight and decomposition length. This provides symmetry: $d(A, B) = d(B, A)$. The triangle inequality is more involved to check.

We have that $A^{-1}C = A^{-1}BB^{-1}C$, and the weight of $A^{-1}C$ is seen to be bounded above by the sum of the weights of $A^{-1}B$ and $B^{-1}C$. Whence $d(A, C) \leq d(A, B) + d(B, C)$ for distance based on weight. Considering the distance based on decomposition length, $A^{-1}B = \prod h^{\sigma_i} \sigma_A$ and $B^{-1}C = \prod h^{\sigma_j} \sigma_B$. Thus we find that $A^{-1}C = \prod h^{\sigma_i} \prod h^{\sigma_A \sigma_j \sigma_A^{-1}} (\sigma_A \sigma_B)$ and this provides an upper bound to the decomposition length. Again the triangle inequality is obtained. In either case we have a metric. \square

3.2 The Main Theorem as an Algorithm

We can analyze the method of the proof to come up with an upper bound for a running time of an algorithm which implements the result. This is the same as

finding an upper bound for the distance in the coset graph (for the Clifford Group and P_{2N}) to the identity if we only happen to know the weight associated with the matrix. Each iteration in the proof acts on the given matrix with a Clifford operator (specifically a Hadamard operator) conjugated by a permutation matrix (representing a Toffoli operator), with the resulting matrix being a signed permutation matrix. Experimentation shows this to be an extremely crude upper bound. Also, empirical speed tests on large dimensional examples shows this algorithm to be quite fast. It also gives an idea of the distance in the Clifford-Toffoli coset graph an actual quantum operator is from the identity.

Proposition 3.2.1. *For an $n \times n$ matrix with weight w (and n even), an algorithm implementing the method in the proof has running time $O(2^n w)$.*

Proof. For a matrix with weight w , we have that each column has at most weight w . It will take at most w steps to reduce the weight of a selected column to 0. The weight of every other column at worst increases by 1 as the selected column is reduced, thus they each have weight at most $w + w = 2w$ after the selected column is reduced.

By induction we show that after k columns are reduced, the weight of the remaining is at most $2^{k+1}w$. When working on the k^{th} column, $k - 1$ have been reduced to 0 and so we assume to have at most $2^k w$ for the weight of the remaining columns. It takes at most $2^k w$ steps to reduce the newly selected column (respecting the already reduced ones) and the others at worst increase in weight by 1 at each step. Thus, after reducing the k^{th} column, the remaining columns have at most weight $2^k w + 2^k w = 2^{k+1}w$.

The number of steps to reduce the n columns is $w + 2w + \dots + 2^n w = (2^{n+1} - 1)w$. □

Proposition 3.2.2. *Two non-reduced columns in a matrix within $\text{SO}_{2N}(\mathbb{Z}\{1/\sqrt{2}\})$ can be simultaneously reduced by an element H^σ .*

Proof. Suppose the two given columns have column weights w_a and w_b with values a_1, a_2, \dots, a_{2N} and b_1, b_2, \dots, b_{2N} respectively. So $w_a, w_b > 0$. For p and q in $\{0, 1\}$, let $Y_{p,q} = \{i \mid \bar{a}_i = p \pmod{2} \text{ and } \bar{b}_i = q \pmod{2}\}$. As the first column is not reduced $\sum_{i=1}^{2N} \bar{a}_i = 2^{w_a}$ and so $\sum_{i=1}^{2N} \bar{a}_i = 0 \pmod{2}$. This gives that the number of $\bar{a}_i = 0$ (or 1) $\pmod{2}$ is even and thus the sizes of $Y_{0,0} \cup Y_{0,1}$ and $Y_{1,0} \cup Y_{1,1}$ are even. Similarly the number of elements in $Y_{0,0} \cup Y_{0,1}$ and $Y_{1,0} \cup Y_{1,1}$ are even.

By orthogonality, $\sum_{i=1}^{2N} a_i b_i = 0$ and so $\sum_{i=1}^{2N} \bar{a}_i \bar{b}_i = 0$. Taken modulo two, one sees that $Y_{1,1}$ has an even number of elements. Immediately one gets that $Y_{0,0}, Y_{0,1}, Y_{1,0}, Y_{1,1}$ all have an even number of elements. A permutation σ may be chosen which creates a pairings contained within each $Y_{p,q}$. □

This improvement shows that an algorithm can be constructed with a running time of $O(2^{n/2} w)$ on $n \times n$ matrices, following a similar argument. Another observation is that when only 4 or fewer columns remain to be reduced, these columns have column weight at most 2. Consider 4 integers modulo 8, the sum of squares of which are 0. Then they must all be 0 modulo 8, and thus multiples of 4. Such numbers cannot represent a reduced column.

Note that this analysis has nothing to do with the Church-Turing Thesis - it is a self-contained measure of complexity. Decomposing a quantum operator or even

using the decomposition to act on a vector will always involve a column with 2^{2N} numbers. To have a relation to the Church-Turing Thesis, these operations would have to be polynomial in N .

Here is some data obtained by decomposing 10,000 randomly created matrices in $\text{SO}_{2N}(\mathbb{Z}[1/2]).\langle H \rangle$. Under random permutations σ , products of H^σ were obtained having a specified weight. Then the algorithm described above is utilized. At the time of choosing a column to reduce, one of minimum weight is selected. This column is then paired with another and both are reduced simultaneously, switching the second column if necessary. The results give how many times a decomposition length was obtained for a random matrix of a specific weight.

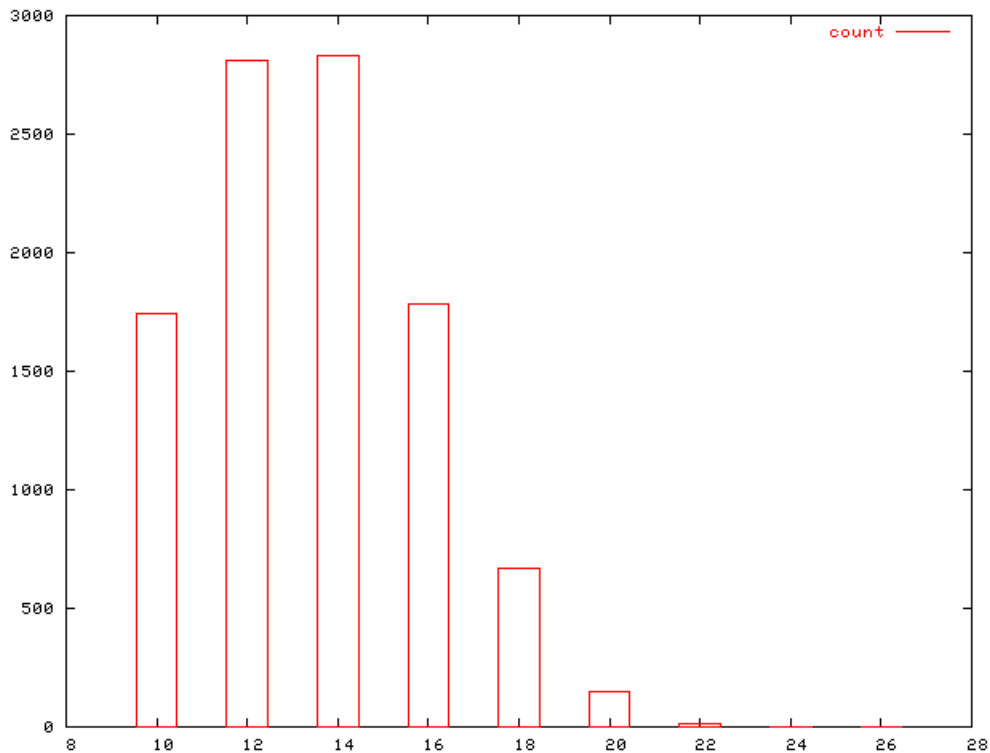


Figure 3-1: Decomposition Length of 10,000 random 8×8 matrices of weight 10

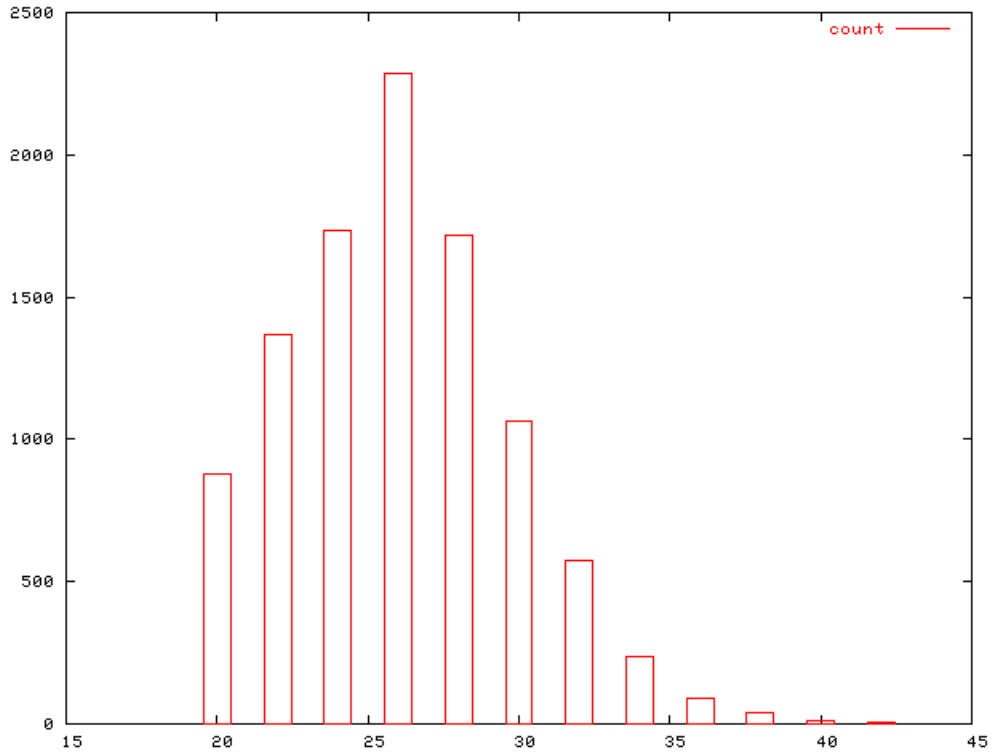


Figure 3-2: Decomposition Length of 10,000 random 8×8 matrices of weight 20

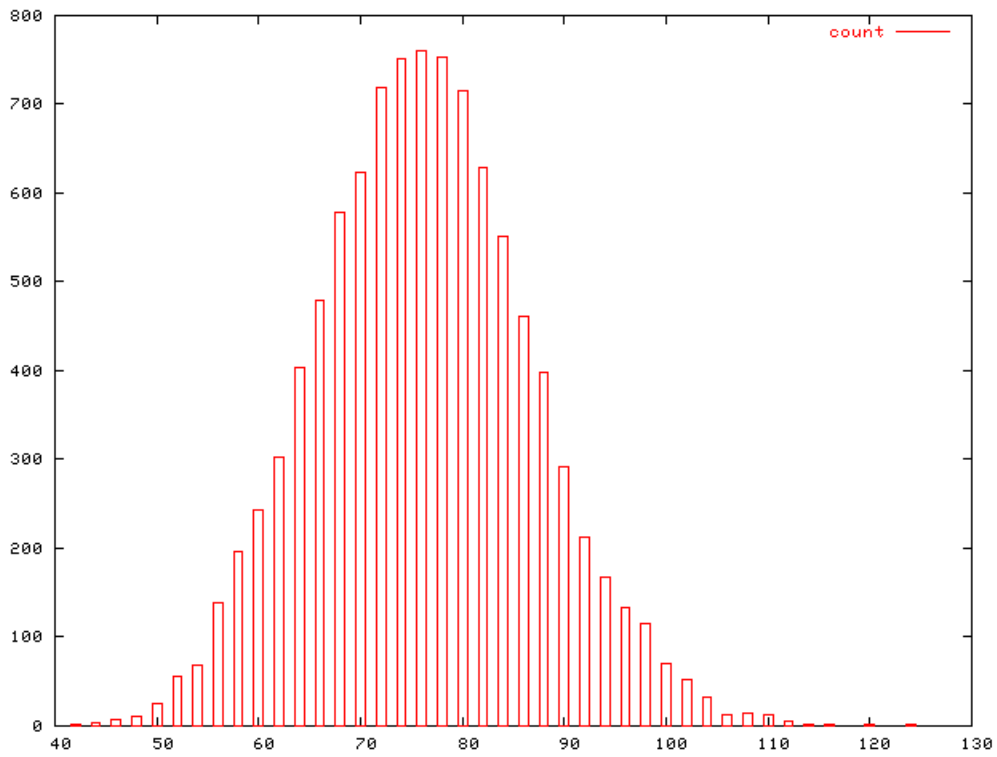


Figure 3-3: Decomposition Length of 10,000 random 16×16 matrices of weight 10

3.3 Normalizers

Fix a positive integer N . Let P (earlier called P_{2N}) be the elements of weight 0 in $\mathrm{SO}_{2N}(\mathbb{Z}\{1/\sqrt{2}\})$. This is the subgroup of signed permutations of determinant 1. Let \hat{P} be the intersection of P and all unsigned permutations. Thus \hat{P} is the permutation representation of the alternating group on $2N$ elements. Note that one of the results is proved in two dramatically different ways.

Proposition 3.3.1. *For $2N \geq 8$, \hat{P} and P are self-normalizing in $\mathrm{SO}_{2N}(\mathbb{Z}\{1/\sqrt{2}\})$.*

Proof. The standard frame, $F = \{\langle e_1 \rangle, \langle e_2 \rangle, \dots, \langle e_{2N} \rangle\}$, is stabilized by the monomial matrices (which are the diagonal matrices times permutation matrices) in $\mathrm{GL}_{2N}(\mathbb{R})$. Restricting this stabilizer to $\mathrm{SO}_{2N}(\mathbb{Z}\{1/\sqrt{2}\})$ gives P .

If $x \in N(P)$, where $N(P)$ is the normalizer of P , then P stabilizes the frame $x \cdot F$. This is because $PxF = xPx^{-1}xF = xF$. The aim is to show that P only stabilizes F , so that P is self-normalizing.

First we find which one dimensional subspaces are preserved by \hat{P} , and use $n = 2N$. Let $v = a_1e_1 + a_2e_2 + \dots + a_n e_n$ be an element in such a space. As \hat{P} is transitive on the standard basis, we see that $a_1 = a_2 = \dots = a_n$. Hence there is but one fixed one dimensional subspace which is preserved by \hat{P} , namely $\langle e_1 + e_2 + \dots + e_n \rangle$. Pick a non-zero vector in this space and call it \tilde{v} .

Let F' be the frame $\{\langle w_1 \rangle, \langle w_2 \rangle, \dots, \langle w_n \rangle\}$, which is stabilized by \hat{P} . On this frame, \hat{P} has orbits O_1, O_2, \dots, O_k . As $n \geq 8$, $\hat{P} \cong \mathrm{Alt}(n)$ is simple. The kernel of \hat{P} acting on O_1 is either trivial or the full group. If the kernel is trivial, then O_1 is the full frame. This is since if O_1 contains j subspaces, then $|\hat{P}| \leq j!$, so j must be

n . If the kernel is the full group, then O_1 has but one subspace. Thus all orbits are trivial, as the other O_k cannot have n elements. This contradicts the space having only a single one dimensional subspace fixed by \hat{P} . Therefore \hat{P} acts faithfully on F' .

The automorphism group for $\text{Alt}(n)$ is $\text{Sym}(n)$ for $n \geq 8$, so we can reorder F' so that the action on the indices coincides with that on the indices of $\{e_1, e_2, \dots, e_n\}$. Let $w_i = a_1^{(i)}e_1 + a_2^{(i)}e_2 + \dots + a_n^{(i)}e_n$. The subgroup stabilizing index 1 will fix e_1 and w_1 . As it is transitive on the rest of the indices, we see that $a_2^{(i)} = \dots a_n^{(i)}$. By scaling, we have that $w_1 = ae_1 + b\tilde{v}$. In general $w_i = e_i + b\tilde{v}$, after scaling (as the coefficient of e_i being 0 does not give a basis of the space).

Consider a linear transformation $x \in \text{SO}_{2N}(\mathbb{Z}\{1/\sqrt{2}\})$ for which $F' = xF$. Up to a coset of \hat{P} , x has one of two forms. The first maps e_i to $\alpha_i w_i$, the second does the same but switches the first and second index. In either case, we have row orthogonality in the matrix x . So, for each i, j , we have that $0 = \alpha_i \alpha_j (2b(1+b) + (n-2)b) = \alpha_i \alpha_j b(2b+n)$. Each α_i cannot be 0, and if $b = 0$ then the frame F' is the standard frame. We must show that $b = -n/2$ cannot occur. Again, using row orthogonality, we see that $1 = \alpha_i^2((1+b)^2 + (n-1)b) = \alpha_i^2(1+2b+nb^2) = \alpha_i^2(1-n+n^3/4)$. We must have $\alpha_i b$ and $\alpha_i(1+b)$ as elements of $\mathbb{Z}\{1/\sqrt{2}\}$, so each α_i is also. For n even, $1-n+n^3/4$ is an integer which is relatively prime to 2, and so its reciprocal is not an element of $\mathbb{Z}[1/2]$.

Now we consider the signed matrix p in P such that $p(e_1) = -e_2$ and $p(e_2) = e_1$, where all other standard basis vectors are fixed. So, $p(w_1) = p(e_1 + b\tilde{v}) = p((1+b)e_1 + be_2 + be_3 \dots be_n) = -e_2 - 2be_2 + b\tilde{v}$. This can only be in some $\langle w_i \rangle$ if $b = 0$. This leads to $a = 0$ (for distinctness) and thus F' is the standard frame,

F . □

Fix a positive integer N . Let P^* be the elements of weight 0 in $O_{2N}(\mathbb{Z}\{1/\sqrt{2}\})$. This is the signed permutation group. Similarly, let P continue to be the elements of weight 0 in $SO_{2N}(\mathbb{Z}\{1/\sqrt{2}\})$. This is the subgroup of signed permutations of determinant 1, also called P_{2N} .

Proposition 3.3.2. *P^* is self-normalizing in $O_{2N}(\mathbb{Z}\{1/\sqrt{2}\})$. P is self-normalizing in $O_{2N}(\mathbb{Z}\{1/\sqrt{2}\})$. P is self-normalizing in $SO_{2N}(\mathbb{Z}\{1/\sqrt{2}\})$.*

Proof. We only prove the third claim, all others are similar. Here, for brevity, we set the normalizer of P as $N(P) = N_{SO_{2N}(\mathbb{Z}\{1/\sqrt{2}\})}(P)$.

Let $p_{(a,b)}$ be the matrix permutation which switches rows (or columns) a and b . Let p_{-a} be the diagonal matrix with entries “1” except for the a , a -th entry which is “-1”.

Pick $m \in O_{2N}(\mathbb{Z}\{1/\sqrt{2}\})$. We wish to show that m has weight 0. $m = 2^{-w/2}X$ where w is the weight of m and X is a (necessarily reduced) integer matrix.

Consider $(p_{-a}p_{(a,b)})^m = m^{-1}p_{-a}p_{(a,b)}m = m^{\text{tr}}p_{-a}p_{(a,b)}m$ in the case where the weight of m is positive. The weight of this matrix is at most $2w$. Now let $Y = X^{\text{tr}}p_{-a}p_{(a,b)}X - X^{\text{tr}}X$. Then $Y_{i,j} = -(X_{a,i} - X_{b,i})(X_{a,j} - X_{b,j}) + 2X_{a,i}X_{b,j}$. So $(p_{-a}p_{(a,b)})^m$ has weight exactly $2w > 0$ iff Y has an odd entry (as $(p_{-a}p_{(a,b)})^X = 2^w I + Y$ and we are taking $w > 0$). This occurs iff $X_{a,i} - X_{b,i}$ is odd for some a, b, i (as the integer matrix will have an odd entry at the i, i -th position).

So, if $m \in N(P)$, then m has weight 0 or $X_{a,i} - X_{b,i}$ is always even for every $0 \leq a, b, i \leq 2N$. In the latter case, it must happen that X is a matrix of all odd

entries, and thus the weight must be at least $4N$. This is because the weight can be found by the inner product of a row with itself and no row has a zero entry in this case.

Now consider $(p_{-a}p_{-b})^m$, with $a \neq b$ and $m \in N(P)$. Let $Z = X^{tr}p_{-a}p_{-b}X - X^{tr}X$. Then $Z_{i,j} = -2X_{a,j}X_{b,j}$ and $(p_{-a}p_{-b})^X = 2^w I + Z$. If the weight of m is positive, then for $(p_{-a}p_{-b})^m$ to have weight 0 it must be the case that 2^w divides Z . But 2^1 exactly divides Z as X has all odd entries. Hence if the weight of m is positive, it must be both 1 and also larger than $2N$, a contradiction.

Hence, if $m \in N(P)$ then m has weight 0. If m has weight 0, then $m \in P \subset N(P)$. Therefore P is self-normalizing in $\mathrm{SO}_{2N}(\mathbb{Z}\{1/\sqrt{2}\})$. \square

As a corollary to both of these propositions, the same self-normalizing results for (possibly signed) elements of weight 0 are also true of the groups $\mathrm{SO}_{2N}(\mathbb{Z}[1/2]) \cdot \langle H \rangle$, $\mathrm{SO}_{2N}(\mathbb{Z}[1/2])$, and the group of quantum operators.

Chapter 4

Quadratic Forms over \mathbb{Q}_2

With the knowledge from the Main Theorem that the group of quantum operators is embedded in $\mathrm{SO}_{2N}(\mathbb{Z}[1/2]).\langle H \rangle \subset \mathrm{SO}_{2N}(\mathbb{Z}\{1/\sqrt{2}\})$, we might attempt to understand it better by considering properties of an overgroup. Motivated by a paper of Kantor[8] which studies some orthogonal groups over $\mathbb{Z}[1/2]$, we too shall investigate vector spaces over the 2-adic field \mathbb{Q}_2 . The goal here is to find a change of basis in such a vector space from the standard sum-of-squares, which the groups respect, to a skew form which is easier to work with.

4.1 P-adics

Along with the reals, which are the completion of the rationals under the standard norm, another type of completion gives a collection of values which are useful in many number theoretic applications. As well as the standard norm, the rationals have a family of norms each based on a fixed prime p . For an integer m , let $o_p(m)$ be the

largest integer k such that p^k divides m . For a reduced fraction of integers $\frac{m}{n}$, we define the p -adic norm $|\cdot|_p$ to be $|\frac{m}{n}|_p = o_p(n) - o_p(m)$. Not only is the p -adic norm an actual norm, it satisfies a stricter condition which makes it a non-Archimedean norm: for each pair of rationals x and y , $|x + y|_p \leq \max(|x|_p, |y|_p)$. The p -adic numbers are the completion of the rationals under this norm (for a fixed p), and are denoted \mathbb{Q}_p .

We would next like to see that p -adics can be expressed in a nice form. For any $x \in \mathbb{Q}_p$, let $m = |x|_p$, then x can be represented by $b_0p^{-m} + b_1p^{-m+1} + \dots + b_{m-1}p^{-1} + b_m + b_{m+1}p + \dots$, where each b_i is an integer in $\{0, 1, 2, \dots, p-1\}$. See [9] for details. The p -adic integers \mathbb{Z}_p are the p -adic numbers with no fractional part, and are equal to $\{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$. We can recognize addition, subtraction and multiplication on the p -adic integers, and extend them to all p -adic numbers if we first factor out from those numbers an appropriate power of p . The values of $x + y$, $x - y$, and xy can be determined by doing the standard algorithms base p , but on values of possibly infinite length. Indeed, restricting $\mathbb{Z}_p \bmod p^m$ for a positive m is a ring homomorphism.

4.2 Quadratic Forms

Fix a field k , and a vector space V over k . A map $f : V \times V \rightarrow k$ is bilinear if for each $x, y, z \in V$, and $\alpha \in k$ $f(\alpha x + z, y) = \alpha f(x, y) + f(z, y)$ and $f(x, \alpha y + z) = \alpha f(x, y) + f(x, z)$. The map is said to be symmetric if $\forall x, y \in V$ we have $f(x, y) = f(y, x)$. The map is said to be skew symmetric if $f(x, y) = -f(y, x)$ under the same conditions. The space V is said to be orthogonal with respect to f if f is symmetric, and symplectic if f is skew symmetric. We will be interested in a certain

symmetric map.

Two vectors x and y are said to be orthogonal when $f(x, y) = 0$. For a subspace W of V , we define its orthogonal complement W^\perp as the collection of all vectors orthogonal to every vector of W , $W^\perp = \{x \in V \mid f(x, y) = 0, \forall y \in W\}$. Observe that W^\perp is itself a subspace of V . We call V^\perp the radical of V . It is the collection of vectors which are orthogonal to every vector in V . We are most interested when $V^\perp = 0$, and when this occurs we say that f is non-degenerate.

A vector x is said to be isotropic if $f(x, x) = 0$. A subspace W is said to be totally isotropic if $f(x, y) = 0$ for each x and y in W . In other words, W is a totally isotropic subspace if $W \subseteq W^\perp$. A subspace W is nondegenerate if its radical is 0, in other words $W \cap W^\perp = 0$ in V .

A quadratic form on V is a map $Q : V \rightarrow k$ such that for each $x \in V$ and $\alpha \in k$, $Q(\alpha x) = \alpha^2 Q(x)$ and $Q(x + y) - Q(x) - Q(y)$ is a symmetric bilinear form. Conversely, if f is a symmetric bilinear form, then $f(x, x)$ is a quadratic form. If we set $f(x, y) = Q(x + y) - Q(x) - Q(y)$, then $Q(x) = f(x, x)/2$. Hence we have a bijection between symmetric and bilinear forms when the characteristic of the field is not 2. When the characteristic of the field is 2, then there are distinct quadratic forms which have an equivalent symmetric bilinear form. In this case it is better to consider a space V as an orthogonal space with respect to the quadratic form Q .

A vector $x \in V$ is said to be singular if $Q(x) = 0$. The subspace W of V is said to be totally singular if W is totally isotropic and each vector in W is singular. If Q has an associated symmetric form, then being singular is equivalent to being isotropic, and being totally singular is equivalent to being totally isotropic. The Witt index of

V with respect to Q is the maximum dimension among all totally singular subspaces of V .

Pick a basis for the space over which the bilinear form f acts $\{v_1, v_2, \dots, v_n\}$. Let \hat{Q} be the matrix with entry $f(v_i, v_j)$ in the $(i, j)^{\text{th}}$ position. Then, with vectors represented in this basis as $n \times 1$ column matrices, one can check that $f(x, y) = x^T \hat{Q} y$. Note that if f is a symmetric form then the matrix \hat{Q} is a symmetric matrix, and if f is a skew form then \hat{Q} is a skew symmetric matrix. Thus the related quadratic form Q has the form $Q(x) = f(x, x) = x^T \hat{Q} x$.

The discriminant $d(Q)$ of a quadratic form Q is the determinant of the associated matrix. If P is an invertible matrix which is being used to change the basis for the form then the associated matrix changes with respect to P . If $y = Px$ then we have that $x^T \hat{Q} x = y^T P^{-T} \hat{Q} P^{-1} y$ and so the new matrix under the change of basis is $(P^{-1})^T \hat{Q} P^{-1}$. So the discriminant under the new basis is $\det((P^{-1})^T \hat{Q} P^{-1}) = \det(\hat{Q}) \det(P^{-1})^2$. This tells us that the discriminant is unique in k/k^2 , that is, unique up to a square. If the discriminant is 0, then the row rank is strictly smaller than the $\dim(V)$. Hence one can find a vector y which is orthogonal to the row space, in other words $\hat{Q}y = 0$. Thus $f(x, y) = 0$ for every x and $\text{rad}(V) = V^\perp$ is non-trivial and the form is degenerate. It can be checked that the discriminant being non-zero is equivalent to the form being non-degenerate. We are interested in the non-degenerate case and thus consider discriminants within $k^*/(k^*)^2$.

Matrices A for which $Q(x, y) = Q(Ax, Ay) \forall x, y \in V$ are matrices which preserve the quadratic form. Under the matrix form, it is necessary and sufficient that $\hat{Q} = A^T \hat{Q} A$. If the form is non-degenerate, then the discriminant of Q is not 0 so $1 =$

$\det(A)^2$. So in particular A is invertible. It is straightforward to check that, in this case, the set of matrices which preserve the form is a group. For familiar forms, these lead to familiar groups such as the orthogonal groups, unitary groups, and symplectic groups.

One interest we have is when two quadratic (or symmetric bilinear) forms are the same form up to a change of basis. Surely then, they must have the same invariants (such as the discriminant) if they are the same. Over \mathbb{Q}_2 , it happens that it is necessary and sufficient for two forms to be equivalent that only a few invariants are identical ([10] page 39). These other invariants involve the Hilbert symbol.

The Hilbert symbol (a, b) , much like the well known Legendre symbol, tells us when a certain quadratic equation has a solution. When $z^2 = ax^2 + by^2$ has a solution in $k^3 - (0, 0, 0)$, then $(a, b) = 1$. It has the value -1 otherwise. Over the 2-adics, there is an equation for computing the Hilbert symbol. To compute it, we need to define two further functions on odd integers:

$$\epsilon(n) = \frac{n-1}{2} \pmod{2} = \begin{cases} 0 & n \equiv 1 \pmod{4} \\ 1 & n \equiv 3 \pmod{4} \end{cases}$$

$$\omega(n) = \frac{n^2-1}{8} \pmod{2} = \begin{cases} 0 & n \equiv \pm 1 \pmod{8} \\ 1 & n \equiv \pm 3 \pmod{8} \end{cases}$$

These arise in the Legendre symbol for determining whether -1 and 2 are quadratic residues. For $a, b \in \mathbb{Q}_2$, $a = 2^\alpha u$ and $b = 2^\beta v$ where u and v are 2-adic units. If $u = 1 + q_1 2^1 + q_2 2^2 + \dots$ is a 2-adic unit then ϵ and ω are computed using the same

formulas. Explicitly, $\epsilon(u) = q_1 \pmod{2}$ and $\omega(u) = q_1 + q_2 \pmod{2}$. The formula for the Hilbert symbol on $a, b \in \mathbb{Q}_2$ is ([10] page 20):

$$(a, b) = (-1)^{\epsilon(u)\epsilon(v) + \alpha\omega(v) + \beta\omega(u)}$$

4.3 Moving Between Forms

There are two symmetric forms which we are interested in. Both are known as orthogonal forms. In an n dimensional space, the form $f(x, y) = \sum_{i=1}^n x_i y_i$ is the standard sum-of-squares form which is familiar. The associated matrix \hat{Q} is the identity matrix in this case. The associated matrix group is the standard orthogonal group, for which $I = A^T A$ which is derived from the earlier discussion. Notice that the group of quantum operators generated by Clifford and Toffoli groups is the collection of matrices with entries in $\mathbb{Z}[1/2]$ which preserve this form (by the Main Theorem). The other orthogonal form of interest in n dimensional space is similar to the symplectic form on the surface. The dimension of the space must be even, and one selects a basis $\{e_1, e_2, \dots, e_m, f_1, f_2, \dots, f_m\}$ where $f(e_i, e_j) = f(f_i, f_j) = 0$ and $f(e_i, f_j) = \delta_{i,j}$. The associated $2m \times 2m$ matrix with this form is:

$$\hat{Q} = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}$$

Under the change of basis $v_i = \frac{1}{2}(e_i + f_i)$, $v_{m+i} = \frac{1}{2}(e_i - f_i)$ one can check that $f(v_i, v_j) = 0$ if $i \neq j$ (hence the familiar orthogonality is present) and that $f(v_i, v_i)$

is 1 for $i \leq m$ and is -1 otherwise. This is only possible if the field is not characteristic two, so the previous definition is more general. Under the more general form, geometries are easier to study.

We would like to know when these two forms are equivalent over \mathbb{Q}_2 . One immediate restriction is that we must use an even dimensional vector space. As $\frac{1}{2}$ is an element of \mathbb{Q}_2 , we can assume the second form for the later symmetric bilinear form. The associated matrix in the sum-of-squares form (call it Q_1) is the identity matrix, and is a diagonal matrix with an equal number of 1's and -1 's in the case of the other form (henceforth Q_2).

Lemma 4.3.1. *The two forms, Q_1 and Q_2 are equivalent forms on a vector space of dimension n over \mathbb{Q}_2 if and only if 8 divides n .*

Proof. Let $n = 2m$. If $\bar{v} = \{v_1, v_2, \dots, v_n\}$ is an orthogonal basis for $V = \mathbb{Q}_2^n$, $\hat{\epsilon}(\bar{v}) = \prod_{i < j} (Q_{i,i}, Q_{j,j})$, where the latter is using the Hilbert symbol.

Theorem 7 in Serre for forms over \mathbb{Q}_p ([10] page 39):

Two quadratic forms over k are equivalent if and only if they have the same rank, same discriminant, and same invariant ϵ .

Under both forms, the rank is n . In either case, any vector orthogonal to a basis element v_i is a linear combination of the other basis vectors. Thus any vector orthogonal to all of them must be the zero vector and hence $V^\perp = \{0\}$. The rank is equal to the codimension of the radical, and so must be n .

The discriminant for Q_1 is just $\det(I) = 1$. As half of the diagonal elements in the associated matrix form for Q_2 have -1 entries, its discriminant is $\det(\hat{Q}_2) =$

$(-1)^{n/2} = (-1)^m$. This invariant is equal for the two forms when 2 divides m .

To compute the $\hat{\epsilon}$ invariant we need to compute the Hilbert symbols in a few cases. We have that $1 = 2^0 1$ and $-1 = 2^0(-1)$ (or $2^0(1 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3 + \dots)$). Furthermore, $\epsilon(1) = 0, \epsilon(-1) = 1, \omega(1) = 0, \omega(-1) = 0$. So, using the definition of the Hilbert symbol, we see that: $(1, 1) = (1, -1) = (-1, 1) = 1$ and $(-1, -1) = -1$. On the first form, $\hat{\epsilon}$ has the value 1. On the second form, $\hat{\epsilon}(\bar{v}) = \prod_{i < j} (Q_{i,i}, Q_{j,j}) = \prod_{m < i < j} (-1) = (-1)^{\frac{m(m-1)}{2}}$. This value is 1 when 4 divides m or 4 divides $m - 1$.

The rank is always equal and all invariants match only when 4 divides m . Thus the forms are equivalent precisely when 8 divides n . \square

Working one subspace at a time, we will be able to find a change of basis between the forms Q_1 and Q_2 . We've already seen a change of basis which takes the symplectic-like form to its orthogonal version. The above Lemma 4.3.1 shows that we need only worry about dimensions which are a multiple of 8, and so if we can find a change of basis in 8 dimensions then we can do it for all cases. Converting it to the sum-of-squares form is done by recursively dividing the space into orthogonal 1 and $n - 1$ dimensional spaces, with the form restricted to each. Finding the one dimensional subspace amounts to finding a vector x such that $Q(x) = f(x, x) = 1$ (in our case). We can reduce ourselves to looking for vectors which represent 1 as the sum-of-squares form has n orthogonal vectors which do so. We have that $f(v_1, v_1) = f(v_2, v_2) = f(v_3, v_3) = f(v_4, v_4) = 1$, so 4 of the 8 dimensions are already taken care of.

Lemma 4.3.2. *If $a \equiv 1 \pmod{8}$, then a has a square root in the 2-adics.*

Proof. If it has a square root in the integers, we are done. Let $a = 1 + 8b$. Since a is odd modulo 2^n with $n \geq 1$, any prospective square root should be of the form $2k + 1$. Attempting to solve $(2k + 1)^2 = 1 + 8b$ modulo a large power of 2 leads to the equation $4(k^2 + k - 2b) = 0$.

We now make use of this equation to find a sequence convergent in the 2-adics which satisfies the equation for ever-increasing powers of 2. Let $k_0 = 0$. Given k_i , set $2^{n_i} s_i = k_i^2 + k_i - 2b$ where s_i is odd and let $k_{i+1} = k_i + 2^{n_i}$. Then $k_{i+1}^2 + k_{i+1} - 2b = 2^{n_i} s_i + 2^{n_i+1} k_i + 2^{2n_i} + 2^{n_i} = 2^{n_i} (s_i + 2k_i + 2^{n_i} + 1)$. Now, as s_i is odd, $s_i + 1$ is even. Also 2^{n_i} is even, even when $k_i = 0$ as we assume $k^2 + k - 2b = 0$ has no solution k in the integers. Hence the equation is congruent to 0 for a larger power of 2 for k_{i+1} than for k_i . If $x_i = 2k_i + 1$, then $|x_i^2 - a|_2 = 2^{-2-n_i}$ and $\{x_i\}$ is a Cauchy sequence (as we are only adding powers of 2). Hence the sequence converges to a square root of a . \square

A specific solution to $-x_5^2 - x_6^2 - x_7^2 - x_8^2 = 1$ is $Z_1 = (1, 1, 2, \sqrt{-7})$. Here we used that -7 has a square root in the 2-adics (and is equal to $2^0 + 2^2 + 2^4 + 2^5 + 2^7 + 2^{14} + O(2^{15})$). We further set the following mutually orthogonal vectors $Z_2 = (1, -1, \sqrt{-7}, -2)$, $Z_3 = (-\sqrt{-7}, -2, 1, 1)$, and $Z_4 = (-2, \sqrt{-7}, 1, -1)$. Extending these vectors by 4 leading dimensions (and with zero coefficients), we obtain the desired relation that $f(Z_i, Z_j) = \delta_{i,j}$. Alternatively, setting a 4 by 4 matrix B with the values of the Z_i 's gives $B^2 = -I$, or $B^{-1} = -B^T$.

A change of basis matrix for converting the sum-of-squares norm to the skew form

is:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & -\sqrt{-7} & -2 \\ 0 & 0 & 0 & 0 & 1 & -1 & -2 & \sqrt{-7} \\ 0 & 0 & 0 & 0 & 2 & \sqrt{-7} & 1 & 1 \\ 0 & 0 & 0 & 0 & \sqrt{-7} & -2 & 1 & -1 \end{pmatrix}$$

This change of basis can also be used in the p -adics for $p \neq 2$ when -7 is a residue mod p . This follows directly from Hensel's Lemma. The times for which -7 is a residue is given by the Legendre symbol $\left(\frac{-7}{p}\right) = \left(\frac{p}{7}\right)$ since $7 \equiv 3 \pmod{4}$ and so when $p \equiv 1, 2, 4 \pmod{7}$.

For the general case of $p \neq 2$, the forms are equivalent in all dimensions divisible by 4. While the above change of basis works for some primes, the restriction to dimensions a multiple of 8 may be inconvenient. The following two change of basis matrices work with the cases in which -1 is a residue (when $p \equiv 1 \pmod{4}$) and respectively when -2 is a residue ($p \equiv 1, 3 \pmod{8}$).

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \sqrt{-1} & 0 \\ 0 & 0 & 0 & \sqrt{-1} \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \sqrt{-2} & -1 \\ 0 & 0 & 1 & \sqrt{-2} \end{pmatrix}$$

Appendix A

Appendix

A.1 Buildings

The goal of this section is to find a structure known as a building associated with the group $\mathrm{SO}_{2N}(\mathbb{Z}[1/2])$. Then, with the thought that the group of quantum operators is near its overgroup $\mathrm{SO}_{2N}(\mathbb{Z}\{1/\sqrt{2}\})\langle H \rangle$ we would analyze how these operators acted on the discovered building. The affine \tilde{D}_n building is desired as acting on the associated tree structure would provide an interesting metric on the group of quantum operators.

Sadly, this was not to be. What appears here is the background for the subject and framing for the presumed building structure. In the following section the less interesting spherical D_n building is obtained.

A.1.1 Coxeter Groups

Historically, the first studied Coxeter groups were reflection groups, finite groups which are an isometry group for some Euclidean space. These reflection groups consider all systems of n mirrors in n dimensions. In two dimensions, these are kaleidoscopes, and in higher dimensions they are the symmetry groups for regular solids. Coxeter groups are the family of groups which extend reflection groups, without an underlying Euclidean space. Also, Weyl groups of semi-simple Lie algebras are Coxeter groups, which were first studied at about the same time.

Formally, a Coxeter group is a group generated by involutions with certain simple relations. If this set of order two elements is $S = \{s_1, s_2, \dots, s_n\}$, then the group can be written $W = \{S \mid (s_i s_j)^{m_{i,j}} = 1\}$, where $m_{i,j}$ is a positive integer (or infinity). There are no further relations than the collection $(s_i s_j)^{m_{i,j}} = 1$, and any set of relations which lead to a group where the order of $s_i s_j$ is smaller than $m_{i,j}$ is not a Coxeter group.

Focusing on the exponents $m_{i,j}$, we derive the following. First we must have that $m_{i,i} = 1 \forall i$ as $s_i^2 = 1$. Secondly the exponents are symmetric in the indices: $m_{i,j} = m_{j,i}$. To see this, first expand the product, $(s_i s_j)^m = s_i s_j \cdots s_i s_j = 1$, and consider the inverse of the word of elements, $1 = s_j^{-1} s_i^{-1} \cdots s_j^{-1} s_i^{-1}$. As the generating elements each have order 2, the inverse of the element is itself and so $1 = s_j s_i \cdots s_j s_i = (s_j s_i)^m$. Finally, we notice that if $m_{i,j} = 2$, then s_i and s_j commute. This is because $(s_i s_j)^2 = s_i s_j s_i s_j = 1$ implies that $s_i s_j = s_j^{-1} s_i^{-1} = s_j s_i$.

Examples:

- The dihedral groups $D_n = \{s, t | s^2 = t^2 = (st)^n = 1\}$.
- The free product $C_2 * C_2 = D_\infty = \{s, t | s^2 = t^2 = 1\}$.
- The symmetric groups $S_n = \{s_1, s_2, \dots, s_{n-1}\}$, with $s_i = (i, i + 1)$ and $n \geq 2$.
(Here $m_{i,j} = 3$ if $|i - j| = 1$ and is 0 otherwise.)
- The groups of reflections and rotations of regular solids in any dimension are generated by the reflections.

A Coxeter matrix is a matrix M such that $M_{i,j} = m_{i,j}$. Note, that by the above, it is a symmetric n by n matrix with integer (or infinite) entries, where $n = |S|$.

Examples

$$M(D_n) = \begin{pmatrix} 1 & n \\ n & 1 \end{pmatrix}$$

$$M(S_5) = \begin{pmatrix} 1 & 3 & 2 & 2 \\ 3 & 1 & 3 & 2 \\ 2 & 3 & 1 & 3 \\ 2 & 2 & 3 & 1 \end{pmatrix}$$

A Coxeter diagram is a graph with $n = |S|$ nodes which encodes the same information as the Coxeter matrix. In more generality these are known as Dynkin diagrams. Two nodes i and j are connected exactly when $m_{i,j} \geq 3$. If i and j are connected, then the value of $m_{i,j}$ appears above the edge between them when $m_{i,j} \geq 4$. Hence there are no self edges in such a diagram, unjoined generators means that they commute, and unlabeled but joined nodes have a product of order 3.

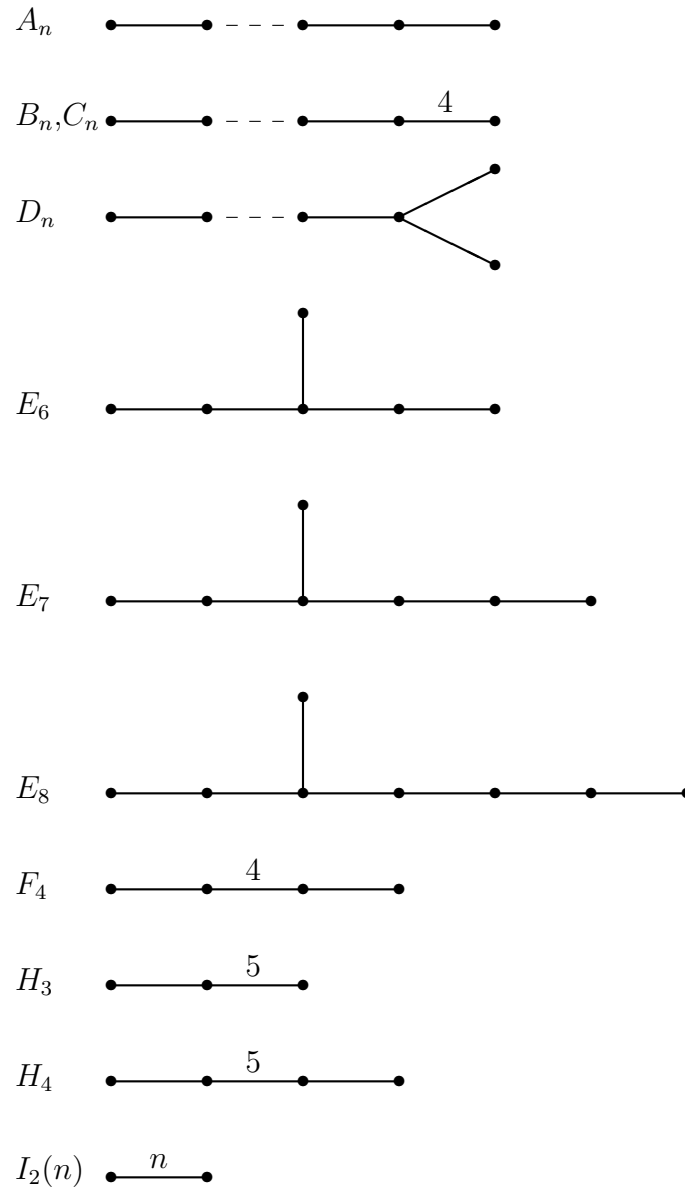


Figure A-1: The list of Coxeter graphs for the finite Coxeter groups

There are other equivalent formulations for Coxeter groups. They focus on the representations of elements in the group by generators. By a word in the generating set S , we mean an ordered sequence $(s_{i_1}, s_{i_2}, \dots, s_{i_m})$ of elements in S . We let w be such a word and write $w = s_1 s_2 \cdots s_m$, where s_j in a word is a shortcut for s_{i_j} as it appears in S . By a reduced decomposition of a word w , we mean an equivalent word representing the same element of the group which is of minimal length. Define $\ell(w)$ to be the length of w represented by any reduced decomposition.

One equivalence of a Coxeter group is a group with the Exchange Condition: given a reduced word $w = s_1 s_2 \cdots s_m$ and $s \in S$, then either $\ell(sw) = \ell(w) + 1$ or there is a deletable index i so that $w = s s_1 s_2 \cdots \hat{s}_i \cdots s_m$ as an element in the group. Another is the deletion condition: given $w = s_1 s_2 \cdots s_m$, if $m > \ell(w)$ then there exists indices i and j such that $w = s_1 \cdots \hat{s}_i \cdots \hat{s}_j \cdots s_m$. Plainly, the deletion condition states that if a word is not reduced then there is a pair of generators which can be removed from a word and the result still represents the same element. The determination of which index/indices can be removed for these conditions is answered by various algorithms.

Because of these properties, Coxeter groups are an example of a group which has a solvable word problem. The word problem in a group is the question of deciding whether a word in terms of the generators of a group is the identity. This can equivalently be stated regarding if two words represent the same element. One must simply apply the deletion algorithm to a word - if it does represent the identity, then all elements will eventually be deleted.

A.1.2 Coxeter Complexes

An idea permeating group actions is that external objects upon which a group acts can be internalized. We will be able to then turn this around and have a generic external object, called a Coxeter complex, which is closely associated to a Coxeter group. Pushing the idea of a Coxeter complex will lead to the notion of a building. Buildings, which require a pairing of a group which acts upon them, provide a wealth of information about the associated group.

For the Coxeter groups which are reflection groups, we begin by considering the natural (or minimal) real vector space on which it acts. Each generator represents the reflection across a hyperplane. Each reflection moves a hyperplane to another hyperplane. Let the orbit of hyperplanes by the Coxeter group (each element thought of as a product of reflections) be H , which will be finite as the group is finite. Each hyperplane in H divides the space into two regions. Consider these two regions as containing the hyperplane, so that the half-spaces are closed.

Define a cell to be any intersection of half-spaces or hyperplanes, one for each hyperplane in H . If the hyperplane itself is chosen each time, then the cell will be a single point (the origin). As otherwise if it were a subspace then the vector space being acted upon is not minimal as this subspace can be quotiented out. On the other extreme, a maximal cell is known as a chamber. Such things are always intersections of half-spaces for each hyperplane in H , although the converse is not true.

Ordered by inclusion, this collection of cells form a simplicial complex. Every cell is a simplex - positive linear sums of vectors within the cell are also contained

in the cell. This property is inherited from the half-spaces and hyperplanes whose intersection is the cell. The number of linearly independent vectors in a cell determine its dimension. The full collection of cells, ordered by inclusion, form a partially ordered set (commonly called poset) where the origin is the smallest of all elements and chambers are the maximal elements. Furthermore, given any two comparable cells, there is a cell between them for every dimension between those of the given cells. This can be accomplished by replacing appropriate half-spaces used in the larger cell's creation with hyperplanes (appropriate meaning that the hyperplane contains the smaller cell).

Now internalize the simplicial complex for reflection groups by looking at the cell stabilizers. All of these stabilizers are conjugate to a group generated by a subgroup of S , the set of involutions which generates the Coxeter group. This is since all hyperplanes can be generated by reflections through the initial hyperplanes. Let a special subgroup of the Coxeter group be any group generated by a subset of S . Every stabilizer of a cell is conjugate to some special subgroup. From the point of view of the special subgroups, each is the stabilizer of some cell. Thus any given cell will include a unique special cell in its orbit. Or, the orbits of the special cells uniquely cover all cells. Internally, the action of the group on an orbit of cells is equivalent to the action on cosets of a cell stabilizer.

For these Coxeter groups which are reflection groups, the simplicial complex is a realization of the Coxeter complex. However, we now have a different set of objects upon which the group acts the same: all cosets of all special subgroups. The origin corresponds to the full group, and chambers all correspond to cosets of the identity

(thus there are as many chambers as there are elements in the group). The partial ordering is carried across and appears as reverse inclusion - one coset as a subset of another is denoted the larger of the two. See [2] for more details on this construction.

Finally, one can see that any Coxeter group has an associated Coxeter complex upon which to act. The collection of all cosets of all special subgroups (ordered by reverse inclusion) behaves, in an abstract way, like the collection of cells for a reflection group. The original terminology is preserved on this object and it too is called a Coxeter complex.

For a Coxeter complex one can associate a distance between two chambers (or cells in the same orbit). Recall that if S is the set of involutions for a Coxeter group satisfying the Coxeter relations, then any word w in S is an ordered string of elements. As Coxeter complexes are transitive on chambers, then for any chambers C and C' there is an element w with $C' = w \cdot C$. The distance between C and C' is then $\ell(w)$, the length of any shortest length word representing the same element as w . It makes sense that infinite Coxeter groups have associated complexes with unbounded distances.

One quite important simplicial complex is a flag complex. Given an incidence geometry of objects of different types, the collection of all possible flags of those objects is the desired flag complex. Here, maximal flags are the chambers for the complex. Unfortunately not all simplicial complexes can be realized as a flag complex, but it is known that all buildings are flag complexes.

A.1.3 Buildings

A building is an object which builds upon the concept of the Coxeter complex. It is a union of subcomplexes (called apartments) with the following properties: (1) each apartment is a Coxeter complex, (2) for every two simplices in the building there is an apartment which contains them, and (3) any two apartments satisfying the second property are isomorphic, and this isomorphism fixes the two simplices. It turns out that any two apartments in a building are isomorphic, and thus the building is associated with a single Coxeter complex. Hence the building is associated with a Coxeter group. Thus if one has a group acting on a simplicial complex providing the isomorphism for the third property (so that one has a building), then there should be a way to associate the related Coxeter group with the group on the building. This will be the focus of this section. Also of note is that the distance between two simplices is well defined, the choice of an ambient apartment does not matter.

The most simple example of a building is a lone Coxeter complex. They are called thin buildings, and anything not thin is called thick. Any co-dimension 1 cell is contained in (is \leq) exactly two chambers; for a thick building the number of chambers will be three or more. Buildings with an associated finite simplicial complex (and thus including thin buildings) are known as spherical buildings. This is because one can think of the finite simplicial cells of a reflection group projected onto the co-dimension 1 sphere for that real vector space. Further families of buildings include affine buildings (which are generally constructed over a field with discrete valuation), Kac-Moody buildings, and Moufang buildings. Lastly, it can be shown that a building

is just a Coxeter complex if and only if the diameter (the maximal distance attainable among all simplices) is finite.

The action of the group G on the building leads to the concept of the BN-pair. Intuitively, the associated Coxeter group should exist as a section of the group - a quotient of the stabilizer of a complex by the stabilizer of all cells in that complex. Define the subgroup N to be the subgroup of G which preserves some apartment, and B the subgroup which stabilizes a chamber in that apartment (not necessarily fixing the apartment). Their intersection, denoted T , fixes both an apartment and one of its chambers, so as above it must act like the identity on the apartment. T is normal in N , and $W = N/T$ is isomorphic to the expected Coxeter group. Recall that the chamber of a Coxeter complex corresponds to the identity of the group, so that the co-dimension 1 cells to the chamber correspond to (have as stabilizer) groups of order 2. Thus the set of involutions S generating W are discovered.

The choice of letters for some of the subgroups come from how they can arise in certain topological groups. B is often called the Borel subgroup, a maximal connected solvable group, and T a maximal torus. The group W is called the Weyl group, after the groups (which are also Coxeter groups) acting on maximal weight root systems for Lie algebras.

Just as one can determine a Coxeter complex from a Coxeter group, one can find a building for a group G with a BN-pair satisfying certain axioms. Define a parabolic subgroup to be any subgroup of G which contains any conjugate of B . The building for G associated with the BN-pair is the collection of parabolic subgroups, ordered by reverse inclusion. One result of this way of thinking is that a group may have

no associated buildings, or more than one non-isomorphic type of building. Also, finite groups can have BN-pairs, and this has led to results in the classification of finite simple groups. Lastly, one can show that a doubly transitive group is exactly the same as a group with a BN-pair that has a Weyl group generated by a single involution.

A motivating example of a building is the general linear group over the reals. The standard basis for the real vector space is $\{e_1, e_2, \dots, e_n\}$. The spans of non-empty proper subsets of the basis form elements of a geometry, where the type of each element is its dimension. The flag complex of this geometry is an apartment, and the type of each flag is the set of types of the elements it contains. For any other apartment, we can extract a basis $\{f_1, f_2, \dots, f_n\}$. As any change of basis can be found in the general linear group, we see that the group supplies the isomorphism needed for the building axiom.

Anything stabilizing the apartment will form a permutation on cells of the same dimension, as it would permute the flags of type $\{1\}$. Thus the subgroup N can readily be seen to be the collection of monomial matrices, by considering the 1 dimensional cells. Select the stabilized chamber to be the maximal flag including $\langle e_1 \rangle \subset \langle e_1, e_2 \rangle \subset \dots \subset \langle e_1, e_2, \dots, e_{n-1} \rangle$. Then, as each subsequent subspace must be preserved, one can see that B is the upper triangular group of matrices. Now, $T = B \cap N$ is the group of diagonal matrices and N/T is the (full) set of permutation matrices. Hence this building for the real general linear group is associated with the symmetric group on n objects, a building of type A_{n-1} .

We look at one further example, which adds a needed idea on a different type of

geometry which will be utilized. The real orthogonal group is the group which respects the sum-of-squares bilinear form. Under a complex change of basis of a $2n$ -dimensional space it is equivalent to the following form: $\langle e_i, e_{i+n} \rangle = 1$ for $i = 1, 2, \dots, n$ and all other inner products are 0.

Definition 8. *The oriflamme geometry is a geometry on totally isotropic subspaces of dimensions $1, 2, \dots, n - 2$ and two of dimension n (note that $n - 1$ dimensional subspaces are excluded) in a $2n$ dimensional space by asserting that two objects are incident if one is a subspace of the other or if both are n dimensional and have an $n - 1$ dimensional intersection.*

An example of a maximal flag in the oriflamme geometry is: $\{\langle e_1 \rangle, \langle e_1, e_2 \rangle, \dots, \langle e_1, e_2, \dots, e_{n-2} \rangle, \langle e_1, \dots, e_{n-1}, e_n \rangle, \langle e_1, \dots, e_{n-1}, e_{2n} \rangle\}$.

The BN-pair for the oriflamme geometry over SO_{2n} gives a D_n geometry. One can also use the standard incidence geometry on the totally isotropic subspaces. Then for the orthogonal group O_{2n} one gets a B_n geometry.

A.1.4 Buildings over the p -adics

Over an Archimedean field like the reals, buildings can be built using subspaces and containment as the incidence relation. The p -adics are non-Archimedean and thus must be dealt with in a different way.

A lattice in p -adic terms is a subset of a \mathbb{Q}_p vector space which is closed under sums and scalar multiples in \mathbb{Z}_p . We will only consider lattices which have maximal dimension. Every such lattice L has a basis $\{e_i\}_{i=1}^n$ for some n , so that for any vector

$v \in L$ there are scalars $c_i \in \mathbb{Z}_p$ with $v = \sum_{i=1}^n c_i e_i$. Given L , by $p^m L$ we mean the lattice with basis $\{p^m e_i\}_{i=1}^n$. The standard lattice, \mathbb{Z}_p^n , is the p -adic lattice over the standard basis over n dimensions. The following proof is similar to one found in [2].

Proposition A.1.1. *Given any two maximal dimensional lattices L and L' of the same \mathbb{Q}_p vector space, there exists a collection of vectors $\{e_i\}_{i=1}^n$ and scalars $\{p^{m_i}\}_{i=1}^n$ such that $\{e_i\}_{i=1}^n$ is a basis for L and $\{p^{m_i} e_i\}_{i=1}^n$ is a basis for L' .*

Proof. There is a basis for both L and L' , and a change of basis matrix $Q = (q_{i,j})_{i,j}$ between them. The goal will be to transform Q into a monomial matrix by a series of elementary row and column operations. Repeat the following algorithm until the a monomial matrix is obtained.

Find the entry $q_{i,j}$ with smallest norm for which there is a non-zero entry in the same row or column. Then multiply by a series of elementary row operations on the left and column operations on the right so that with the exception of $q_{i,j}$ the i^{th} row and j^{th} column contain all zeros. Rows and columns where this condition already holds will not be altered by matrices operating on different rows and columns. These elementary operations will differ from the identity by an element from \mathbb{Z}_p , since $q_{i,j}$ has smallest norm.

After repetition, we are left with a monomial matrix $M = E_R Q E_C$. Here, E_R is the product of the row operations and E_C the column operations. Thus $Q = E_R^{-1} M E_C^{-1}$. Now, change the basis for L by E_R^{-1} . Since the inverse of each elementary row operation also takes entries in \mathbb{Z}_p , so do E_R and E_R^{-1} and the two bases span the same lattice. Similarly, change the basis for L' by E_C . Then under the new bases,

the change of basis from L to L' is M , a monomial matrix. With a reordering of one of the bases, as well as multiplying by a suitable diagonal matrix with unit entries, the result holds. \square

Two lattices L and L' are said to be equivalent if $L' = p^m L$ for some m . A lattice class is a set of lattices, any two of which are equivalent. By the above proposition A.1.1, the group of automorphisms of a lattice are contained in $\text{SL}(\mathbb{Z}_p)$. The stabilizer of a lattice class is generated by this group as well as integral powers of p times the identity. This motivates the determination of a type for a lattice class. Suppose L is a member of a lattice class, and g is a matrix element which moves the standard lattice \mathbb{Z}_p^n to L by a change of basis. Then define the type of that lattice class to be $o_p(\det(g)) \pmod{p}$. Note that the stabilizer of this class causes the definition to be well defined. Notice that the number of incidence classes is equal to the dimension of the lattices, and that the type of the standard lattice is 0.

For L and L' lattices, say that L is incident to L' if either $pL \subset L' \subset L$ or $pL' \subset L \subset L'$. Note that two lattices of the same type cannot be incident. We say that two lattice classes are incident if from each a member can be provided and these two lattices are incident. Notice that if L and L' are incident by the first relation, then $p^2L \subset pL' \subset pL \subset L'$. Thus pL and L' are incident.

Next we define what it means for two lattice classes to be incident. Suppose that in dimension n we have n distinct lattice classes, one of each possible type, any two of which are incident. We wish to show that there are representatives $L_0, L_1, L_2, \dots, L_{n-1}$ for each lattice class such that $pL_0 \subset L_1, L_2, \dots, L_{n-1} \subset L_0$.

Pick an L_0 from the lattice class of type 0. For each $k \neq 0$ we have a lattice L_k of type k from its lattice class such that either $pL_0 \subset L_k \subset L_0$ or $pL_0 \subset pL_k \subset L_0$ from the definition of incident lattice classes (and the above observation). Choosing L_k accordingly (either the original L_k or pL_k) gives the desired result. Note that the choice of index to use so that pL_i and L_i bound the other lattices was arbitrary.

Consider the lattice quotient L_0/pL_0 . This is isomorphic to the n dimensional vector space over the field of p elements. So for each $k \neq 0$, we have $0 \subset L_k/pL_0 \subset L_0/pL_0$ and L_k/pL_0 is a proper subspace. By proposition A.1.1 under the restriction of the incidence, there is a common basis and collection of scalars so that L_0 has basis $\{f_1, f_2, \dots, f_n\}$ and L_k has basis $\{pf_1, pf_2, \dots, pf_m, f_{m+1}, \dots, f_n\}$. The basis elements form a matrix g taking the standard lattice to the given lattice. So, since

$$o_p(\det([f_1, f_2, \dots, f_n])) \pmod{p} = 0$$

we have that

$$o_p(\det([pf_1, pf_2, \dots, pf_m, f_{m+1}, \dots, f_n])) \pmod{p} = m$$

Thus $k = m$ and for each lattice L_k we have that L_k/pL_k has dimension $n - k$ (or index k in L_0/pL_0). Thus $pL_0 \subset L_{n-1} \subset L_{n-2} \subset \dots \subset L_1 \subset L_0$ and the quotient by pL_0 gives a chain of n subspaces over the field of p elements. This is a description of a maximal flag. Note that with the same basis we could have defined L'_k as having basis $\{\frac{1}{p}f_1, \dots, \frac{1}{p}f_k, f_{k+1}, \dots, f_n\}$ and considered $\frac{1}{p}L_0/L_0$, so that the dimension of L'_k/L_0

is k .

For the remainder of this text we focus on $p = 2$ as we filter the quadratic form through lattice quotients. Given a quadratic form $Q(x)$ call the related quadratic form $\hat{Q}(x)$. For a collection of a chain of lattices which realize a maximal flag of lattice classes, as described above, we have the common set of vectors $\{f_1, f_2, \dots, f_n\}$ and their scalar multiples which are the basis for the lattices. Cover the vectors of $L_0/2L_0$ with the pre-images $\sum_{i=1}^n a_i f_i$ where a_i is either 0 or 1. If the quadratic form $Q(\cdot)$ (or its associated symmetric bilinear form $f(\cdot, \cdot)$) is identically 0 on these vectors then $\hat{Q}(x) \equiv 0$. Otherwise, there is an integer r so that for any one of these 2^n vectors v we have that $2^r Q(v)$ is a 2-adic integer, and at least one is a 2-adic unit. In this case define $\hat{Q}(v) = 2^r Q(v) \pmod{2}$. One may also use $f(x, x)$, which differs from $Q(x)$ by a power of 2, and thus does not affect \hat{Q} .

This definition is well defined as scaling the chosen L_0 by powers of 2 scales the quadratic form on the set of 2^n vectors by the same power of 4. This is since $Q(ax) = a^2 Q(x)$ and the result is shifted to \mathbb{Z}_p . Also if a is a 2-adic integer then $a^2 = 1 + O(2^2)$, so the choice of each f_i is also independent of \hat{Q} . Choosing any other L_0 out of its lattice class will determine the other L_k for each rank and the same set $\{f_1, f_2, \dots, f_n\}$ will result. However, by considering a differently ranked lattice to bookend the others, for example $pL_k \subset L_{k-1} \subset \dots \subset L_1 \subset L_0 \subset L_{n-1} \subset \dots \subset L_k$, we obtain a different \hat{Q} . So it is the case that we will attempt to build a building with quadratic forms based on $L_0/2L_0$.

The orthogonal (symmetric bilinear) sum-of-squares form, $f(x, y) = \sum_{i=1}^n x_i y_i$ (where $x = \sum_{i=1}^n x_i e_i$ and $\{e_i\}$ is the standard basis). It has associated quadratic

form $Q(x) = f(x, x)/2$. If L_0 can be taken as having the standard basis, then for $v = \sum_{i=1}^n a_i e_i$, with a_i either 0 or 1, we have $\hat{Q}(v) = \sum_{i=1}^n a_i \pmod 2$ (or equivalently $\sum_{i=1}^n a_i^2 \pmod 2$).

Here we need to reference the oriflamme (definition 8) geometry of orthogonal forms to investigate the subclass of maximal flags which respect that form. Instead of the sum-of-squares form, we will consider groups, under the change of basis found in a previous section, which respect the equivalent skew form. We will say that the maximal flag respects the form if that form, when filtered through the lattice class quotients as defined above, has the same maximal Witt index.

Is it possible to find a building, and especially one of affine D_n type? If so one can find out how generators and interesting subgroups of the group of quantum operators move the building.

A.2 Reduction Modulo p

When $p \equiv \pm 1 \pmod 8$, 2 is a residue modulo p and so $x^2 - 2$ has two solutions modulo p . Thus we are able, once the choice for $\sqrt{2}$ is made, to embed the group $\langle H^P | P \in P_{2N} \rangle$ within $GL_{2N}(\mathbb{F}_p)$. An immediate consequence of this observation is that $\langle H^P | P \in P_{2N} \rangle$ has infinitely many normal subgroups of finite index. The same is thus also true for $SO_{2N}(\mathbb{Z}\{1/\sqrt{2}\})$. It would be interesting to know what other things can be determined from the finite factor group.

Proposition A.2.1. *All elements of $\langle H^P | P \in P_{2N} \rangle$ of weight less than $\log_2 \frac{\sqrt{p/2}}{2N}$ is faithfully embedded modulo p .*

Proof. Let w_0 be the smallest integer strictly less than $\log_2 \frac{\sqrt{p/2}}{2N}$ and let $2w'_0$ be the largest even integer less than or equal to w_0 . Consider every integer matrix X with $XX^T = 2^{4w'_0}$, recalling that the special orthogonal group is an index two subgroup. No entry of any X will exceed $-2^{2w'_0}$ or $2^{2w'_0}$. So they can be embedded modulo p when $2^{4w'_0} < p$. Note that any matrix M in the group with even weight $w \leq w'_0$ gives us such an $X = 2^{w/2}M$. Conversely, every X gives an element of the group $M = 2^{-w'_0/2}X$.

Now let X be an integer matrix with $XX^T = 2^w$, $w < \log_2 \frac{\sqrt{p/2}}{2N}$. The entries of X are bounded by $\pm \frac{p}{2N}$, and so the entries of X^2 are bounded by $\pm p/2$. Then X^2 is a matrix with even weight and the above is applicable. \square

We will also be able to acquire a D_n diagram quite directly for the index 2 subgroup $SO_{2n}(\mathbb{Z}[1/2])$ by showing that the full orthogonal group over the field of 3 elements is obtained modulo 3. From the sum-of-squares quadratic form having determinant +1, this is the group $O_{2n}^+(3)$. Explicitly, all even dimensional orthogonal groups over a finite field differing only in quadratic form, but having the same determinant, are equivalent. If the factor group of a given group has an associated diagram, then the corresponding subgroups of interest (including B , N , T , and the parabolics) in the original group lead the same building and diagram. This is since the flag complex of parabolic subgroups is acted on exactly the same.

We require the setup used in a paper by Ishibashi and Earnest [7]. The $k + 2$ dimensional vector space over \mathbb{F}_3 decomposes into $H \perp L$ with respect to the quadratic form $Q(x) = f(x, x)$. H is a hyperbolic with basis $\{u, v\}$ and L decomposes into

$\mathbb{F}_3x_1 \perp \mathbb{F}_3x_2 \perp \cdots \mathbb{F}_3x_k$. For $u, v, x_1, x_2, \dots, x_k$ we have $Q(u) = Q(v) = 0$, $f(u, v) = 1$, $Q(x_1) = -1$, and $Q(x_2) = \cdots = Q(x_k) = 1$. These will be explicitly constructed in the upcoming proposition.

Some orthogonal transformations also shall be defined. Δ swaps u and v while fixing every vector in L , and $\phi(-1)$ sends elements in H to their negative while fixing every vector in L . An Eichler transformation $E(u, x)$ is defined for any $x \in L$ by its action on an element z as $E(u, x)z = z + f(z, x)u - f(z, u)x - f(z, u)Q(x)u$. The most important thing to notice about Eichler transformations is that if z is orthogonal to both u and x , then $E(u, x)z = z$.

Proposition A.2.2. $O_{2n}(\mathbb{Z}[1/2]) = O_{2n}^+(3) \pmod{3}$ and $SO_{2n}(\mathbb{Z}[1/2]) = SO_{2n}^+(3) \pmod{3}$ for $n \geq 2$.

Proof. The order of $O_4^+(3)$ is known to be 1152. $O_4(\mathbb{Z}[1/2])$ contains the signed permutation group B_4 , which has exactly one of $\{+1, -1\}$ in each row and column and 0 in every other entry. This subgroup is isomorphic to its image modulo 3, and has $2^4! = 384$ elements. Next, consider elements of $O_4(\mathbb{Z}[1/2])$ with all entries being $+1/2$ or $-1/2$. Modulo 3, $1/2 = 2 = -1$ and $-1/2 = 1$, so these elements are in 1-1 correspondence with their image. Keep the following modulo 3 matrix in mind:

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

Fixing the first row as all 1's, the second (and subsequent) rows need two of both +1 and -1 to remain orthogonal to the first. Choosing where the two 1's land leads to $\binom{4}{2} = 6$ possibilities for the second row. For the third row to be orthogonal to the second, a $\{+1, -1\}$ pair is paired for each pair of the same value in the second row. So, with the first and second row fixed, there are $\binom{2}{1}\binom{2}{1} = 4$ choices for the third row. The fourth row will have only 2 choices for numbers - a row and its negative. Finally, diagonal matrices with $\{+1, -1\}$ entries act on the right to permute all such matrices, in $2^4 = 16$ permutation blocks depending on the values of the first row. Thus, in total, there are $6 \cdot 4 \cdot 2 \cdot 16 = 768$ orthogonal matrices of this form and thus together with B_4 the group has the required number of elements and is $O_4^+(3)$.

For the even dimensions higher than 4 we note that $O_4^+(3)$, extended by the identity, exists as a subgroup of the image modulo 3 since the original elements of interest can be extended by the identity.

Let $\{e_1, e_2, \dots, e_{2n}\}$ be the standard basis, so that $Q(e_i) = 1$ and $f(e_i, e_j) = 0$ for i and j distinct. Define the needed elements $u = e_1 + e_2 + e_3$, $v = e_1 + e_2 - e_3$, $x_1 = e_1 - e_2$ and $x_i = e_{i+2}$ for $2 \leq i \leq 2n - 2$. Check that these satisfy the required conditions. Extend Δ , $\phi(-1)$, and $E(u, x_2)$ as they exist in $O_4^+(3)$ by the identity on the new basis elements, recalling that $E(u, x_2)x_i = x_i$ for $i > 2$.

Define θ by the permutation $x_2 \rightarrow x_3 \rightarrow \dots \rightarrow x_{2n-2} \rightarrow x_2$, which exists in the original group as these x_i 's each are a standard basis element. Next, set $y_2 = x_2 + x_3$

and $y_3 = x_2 - x_3$ and define θ' by $x_1 \rightarrow y_2 \rightarrow y_3 \rightarrow x_1$. Over 6 dimensions, verify that

$$\theta' = \begin{pmatrix} -1 & -1 & 0 & -1 & 1 & 0 \\ -1 & -1 & 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & -1 & -1 & 0 \\ -1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1/2 & 1/2 & 0 & 1/2 & -1/2 & 0 \\ 1/2 & 1/2 & 0 & -1/2 & 1/2 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1/2 & -1/2 & 0 & 1/2 & 1/2 & 0 \\ 1/2 & -1/2 & 0 & -1/2 & -1/2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \pmod{3}$$

and can be extended by the identity as the later x_i elements are e_{i+2} . Thus, by the second case of proposition 3.3 in [7], we generate the full group $O_{2n}^+(3)$. The subgroup of elements of determinant 1 then demonstrate that the full special orthogonal group is present. \square

Note that the proof required modulo 3 operations to show that an orthogonal group could be found for a low dimension. If any orthogonal group can be found for a given prime p then the results of Ishibashi and Earnest say that this group extended by the identity together with a lone permutation will generate the full orthogonal group for any even dimension.

A.3 Source Code

Here, basic source code is provided for decomposing an element in $SO_{2N}(\mathbb{Z}\{1/\sqrt{2}\})$. This is only the basic algorithm, without the discussed speedups. The integer part of the entries is stored in `SOMat`.

```

# PermutationSign

# Follows each cycle and counts the number of transpositions in each

# Returns 0 or 1 depending on if the permutation is even or odd

```

```

def PermutationSign(permutation,N):

```

```

    mark = [0]*N

    transcount = 0;

    for i in xrange(N):

        while mark[i] == 0:

            mark[i] = 1

            i = permutation[i]

            transcount = transcount + 1

            transcount = transcount - 1

    return (transcount % 2)

```

```

# MatrixWeight

```

```

# 2^weight = sum of squares of any row or column

# return the weight

```

```

def MatrixWeight(SOmat, N):

```

```

    sqrsum = 0

    column = 1

    for i in xrange(N):

```



```

    sqrsum = sqrsum + S0mat[i][column] * S0mat[i][column]

weight = 0

while 2**weight <> sqrsum:

    weight = weight + 1

return weight

# ColumnWeight

# Being a column in a matrix means that the entries may be
# inflated by powers of 2, so correct this.

# 2^fullweight = sum of the squares of the column entries
# 2^diff = highest power of 2 dividing all entries in the column
# returns fullweight-diff, which is the weight of just the column

def ColumnWeight(column, S0mat, N):

    sqrsum = 0

    for i in xrange(N):

        sqrsum = sqrsum + S0mat[i][column] * S0mat[i][column]

    weight = 0

    while 2**weight <> sqrsum:

        weight = weight + 1

    diff = 0

    done = 0

    while 1:

```

```

for i in xrange(N):
    if ((S0mat[i][column] >> diff) % 2) <> 0:
        done = 1
    if done == 1:
        break
    diff = diff + 1
weight = weight - 2*diff
return weight

# AdjustMatrix
# After an operation, the matrix may not be reduced.
# Find the largest power of 2 dividing all entries.
# Scale the matrix by this power of 2

def AdjustMatrix(S0mat, N):
    diff = 0
    done = 0
    while 1:
        for i in xrange(N):
            for j in xrange(N):
                if ((S0mat[i][column] >> diff) % 2) <> 0:
                    done = 1

```

```

    if done == 1:
        break

    diff = diff + 1

for i in xrange(N):
    for j in xrange(N):
        S0mat[i][j] = S0mat[i][j] >> diff

def ReduceColumn(column, previouscolumn, needspair, pairs, S0mat, N):
    while ColumnWeight(column, S0mat, N) > 0:
        # Find the highest power of 2 dividing each entry in the column
        diff = 0
        done = 0
        while 1:
            for i in xrange(N):
                if ((S0mat[i][column] >> diff) % 2) <> 0:
                    done = 1
            if done == 1:
                break
            diff = diff + 1
        # Determine the type of row for each element in this column
        # up to the highest power of 2 dividing each entry
        type = ['unk']*N
        for i in xrange(N):

```

```

if ((S0mat[i][column] >> diff) % 2) == 0:
    type[i] = 'even'

if ((S0mat[i][column] >> diff) % 2) == 1:
    type[i] = 'odd'

# Start filling the permutation with already paired rows

permutation = [0]*N

permidx = 0

for i in pairs:
    type[i] = 'paired'
    permutation[permidx] = i
    permidx = permidx + 1

# When working on a column paired with one which has already been
# reduced, the previous column may now be unreduced and have
# entries in 2 rows. This happens every other column reduction.
if needspair and (ColumnWeight(previouscolumn, S0mat, N) <> 0):
    for i in extrapairs:
        type[i] = 'paired'
        permutation[permidx] = i
        permidx = permidx + 1

# Make pairs out of the remaining 'even' and 'odd',
# placing them in the permutation

```

```

for kind in ['even', 'odd']:
    for i in xrange(N):
        if type[i] == kind:
            permutation[permidx] = i
            permidx = permidx + 1

# The extrapairs which will be needed in the next column reduction.
if needspair and (ColumnWeight(previouscolumn, S0mat, N) == 0):
    lonelypair = 0
    while S0mat[lonelypair][previouscolumn] == 0:
        lonelypair = lonelypair + 1
    idx = 0
    while permutation[idx] <> lonelypair:
        idx = idx + 1
    # Find the number next to it in the permutation
    if (idx % 2) == 0:
        matchedpair = permutation[idx+1]
    if (idx % 2) == 1:
        matchedpair = permutation[idx-1]
    extrapairs = [lonelypair, matchedpair]

# If the created permutation is odd, make it even (alternating)
if PermutationSign(permutation, N) == 1:

```

```

temp = permutation[0]

permutation[0] = permutation[1]

permutation[1] = temp

# Apply the hadamard wrt the permutation

permidx = 0

while permidx < N:

    for i in xrange(N):

        temp1 = S0mat[permutation[permidx]][i]
                + S0mat[permutation[permidx+1]][i]

        temp2 = S0mat[permutation[permidx]][i]
                - S0mat[permutation[permidx+1]][i]

        S0mat[permutation[permidx]][i] = temp1

        S0mat[permutation[permidx+1]][i] = temp2

    permidx = permidx + 2

# Remove extra powers of 2

AdjustMatrix(S0mat, N)

# End of main loop - when the column weight is > 0

# When an even number of columns have been reduced, one gets a new

# permanent row pairing

```

```

if needspair:
    lonelypair = 0
    while S0mat[lonelypair][previouscolumn] == 0:
        lonelypair = lonelypair + 1
    pairs.append(lonelypair)

    matchedpair = 0
    while S0mat[matchedpair][column] == 0:
        matchedpair = matchedpair + 1
    pairs.append(matchedpair)

# Given N, the dimension (even)
# Given S0mat, an N by N matrix with the property that
# S0mat * S0mat^T = 2^w * IdentityMat

pairs = []
previouscolumn = -1
needspair = 0
for column in xrange(N):
    ReduceColumn(column, previouscolumn, needspair, pairs, S0mat, N)
    needspair = 1 - needspair
    previouscolumn = column

```

Bibliography

- [1] Ibm's test-tube quantum computer makes history.
http://domino.research.ibm.com/comm/pr.nsf/pages/news.20011219_quantum.html.
- [2] Kenneth S. Brown. *Buildings*. Graduate Texts in Mathematics. Springer-Verlag, 2nd edition, 1989.
- [3] Schor P.W. Sloane N.J.A. Calderbank R.A., Rains E.M. Quantum Error Correction Via Codes over $GF(4)$. arXiv:quant-ph/9608006v5, 1997.
- [4] Stefaan Delcroix and Ulrich Meierfrankenfeld. Locally Finite Simple Groups of 1-Type. *Journal of Algebra*, 247(2):728–746, 2002.
- [5] D. Gottesman. Stabilizer Codes and Quantum Error Correction. Ph.D. thesis, California Institute of Technology, Pasadena, CA (1997). arXiv e-print quant-ph/9705052.
- [6] J. I. Hall. Infinite alternating groups as finitary linear transformation groups. *Journal of Algebra*, 119:337–359, 1988.
- [7] Hiroyuki Ishibashi and A. G. Earnest. Two-element generation of orthogonal groups over finite fields. *Journal of Algebra*, 165(1):164–171, 1994.

- [8] William M. Kantor. Some Exceptional 2-Adic Buildings. *Journal of Algebra*, 92:208–223, 1985.
- [9] Neal Koblitz. *p-adic Number, p-adic Analysis, and Zeta-Functions*. Number 58 in Graduate Texts in Mathematics. Springer, 2nd edition, 1984.
- [10] Jean-Pierre Serre. *A Course in Arithmetic*. Number 7 in Graduate Texts in Mathematics. Springer-Verlag, 1973.