LOWER BOUNDS NON-CLIFFORD RESOURCES

by

Ravi Rai

Submitted in partial fulfillment of the requirements
for the degree of Master of Science

at

Dalhousie University
Halifax, Nova Scotia
August 2021

Optionally, the thesis can be dedicated to someone, and the student can enter the dedication content here.

Table of Contents

Abstract

This is a test document.

Acknowledgements

Thanks to all the little people who make me look tall.

Chapter 1

Introduction

Get it done! Use reference material by Lamport [?] or Gooses, Mittelback, and Samarin [?].

To test if the margins are satisfactory, let us generate a lot of garbage text: This sentence goes on, and on,

and here we should be around top of the page 2, and we go on, and on, and on, and on, and on. This following line ________ should be exactly 5cm long. It can be used to check the typesetting process. And now we go on, and on.

Chapter 2

Basic Techniques

2.1 Stabilizer Nullity

Definition 2.1.1 (Stabilizer)**.** Let $|\psi\rangle$ be a non-zero n-qubit state. The stabilizer of $|\psi\rangle$ is the sub-group of the Pauli group $\mathcal{P}_n$ on n qubits for which $|\psi\rangle$ is a $+1$ eigenstate, denoted by Stab$|\psi\rangle$. This means that Stab$|\psi\rangle = \{P \in \mathcal{P}_n \; P\,|\psi\rangle = |\psi\rangle\}$. The states for which the size of the stabalizer is $2^n$are called stabalizer states. States for which the stabilizer contains only the identity matrix are said to have a trivial stabilizer. If Pauli P is in Stab$|\psi\rangle$, we say that P stabilizes $|\psi\rangle$.

Proposition 2.1.2. *Let $|\psi\rangle$ be a non-zero n qubit state. Then we have the following facts about Stab$|\psi\rangle$:*

1. *Stab$|\psi\rangle$ does not contain -I.*
2. *All Pauli group elements contained in Stab$|\psi\rangle$ commute with each other and are Hermitian matrices.*
3. *The size of the stabilizer is equal to some power of two.*
4. *Given any Clifford Unitary C, the size of Stab$|\psi\rangle$ is always equal to the size of Stab$(C\,|\psi\rangle)$.*
5. *Finally, the size of the stabilizer is multiplicative for the tensor products of states, that is $|Stab(|\psi\rangle\,|\phi\rangle)| = |Stab\,|\psi\rangle\,| \cdot |Stab\,|\phi\rangle\,|$.*

Proof.

1. If $I \in$ Stab $|\psi\rangle$, then $-\,|\psi\rangle = -I\,|\psi\rangle = |\psi\rangle$, which of course is not true for non-zero states.
2. First note that for any two Pauli's P, Q, they either commute or anti-commute. Now suppose $P, Q \in$ Stab $|\psi\rangle$ anti-commute. Then $|\psi\rangle = PQ\,|\psi\rangle = -QP\,|\psi\rangle = -\,|\psi\rangle$.

This implies that $-I \in \text{Stab}\,|\psi\rangle$, which from above can't be true, so P and Q must commute.

3. It is known that the Pauli group's cardinality is a power of two, and since $\text{Stab}\,|\psi\rangle$ is a subgroup of the Pauli group, $|\text{Stab}\,|\psi\rangle\,|$ must divide a power of two, thus it must also be a power of two.

4. First note that Clifford unitaries normalize pauli matrices, i.e. for some Clifford unitary C, and some pauli P, $CPC^\dagger = P'$, where P' is also a pauli. Now let $P \in \text{Stab}\,|\psi\rangle$ and let C be some Clifford unitary. Then $P'C\,|\psi\rangle = CPC^\dagger C\,|\psi\rangle = CP\,|\psi\rangle = C\,|\psi\rangle$, so $P' \in \text{Stab}(C\,|\psi\rangle)$. Now consider the map $\theta_C : \text{Stab}\,|\psi\rangle \to \text{Stab}(C\,|\psi\rangle)$ which takes elements $P \mapsto CPC^\dagger = P'$. This map has an inverse, $\theta_{C^\dagger} : \text{Stab}(C\,|\psi\rangle) \longrightarrow \text{Stab}(C^\dagger C\,|\psi\rangle)$, which takes elements $P' \mapsto C^\dagger P' C$ (where we note that $\text{Stab}(C^\dagger C\,|\psi\rangle) = \text{Stab}\,|\psi\rangle$). Thus θ_C is a bijection, and so we have that $|\text{Stab}\,|\psi\rangle\,| = |\text{Stab}(C\,|\psi\rangle)|$.

5. Let $|\phi\rangle$ be another non-zero state on n qubits, and let $P \in \text{Stab}\,|\psi\rangle$ and $Q \in \text{Stab}\,|\phi\rangle$. Then $P \otimes Q\,|\psi\rangle\,|\phi\rangle = P\,|\psi\rangle \otimes Q\,|\phi\rangle = |\psi\rangle\,|\phi\rangle$. So $P \otimes Q \in \text{Stab}\,|\psi\rangle\,|\phi\rangle$. Now let $R \in \text{Stab}\,|\psi\rangle\,|\phi\rangle$. Then since R is a Pauli, we can write $R = R_1 \otimes R_2$, and $R\,|\psi\rangle\,|\phi\rangle = |\psi\rangle\,|\phi\rangle = R_1 \otimes R_2\,|\psi\rangle\,|\phi\rangle \implies R_1 \in \text{Stab}\,|\psi\rangle$ and $R_2 \in \text{Stab}\,|\phi\rangle$. So every element in $\text{Stab}\,|\psi\rangle\,|\phi\rangle$ is of the form $R_1 \otimes R_2$ as above, thus $\text{Stab}\,|\psi\rangle\,|\phi\rangle = \text{Stab}\,|\psi\rangle \otimes \text{Stab}\,|\phi\rangle$. Then we have a bijection (from the direct product) $\theta : \text{Stab}\,|\psi\rangle \times \text{Stab}\,|\phi\rangle \longrightarrow \text{Stab}\,|\psi\rangle \otimes \text{Stab}\,|\phi\rangle$, which gives us $|\text{Stab}\,|\psi\rangle\,|\phi\rangle\,| = |\text{Stab}\,|\psi\rangle \otimes \text{Stab}\,|\phi\rangle\,| = |\text{Stab}\,|\psi\rangle\,| \cdot |\text{Stab}\,|\phi\rangle\,|$.

$\square$

An example of a stabilizer state is the $|0\rangle$ state, since there are 2^1 pauli's that stabilize it, namely I and Z. Note that for any Clifford C, $|\text{Stab}\,|0\rangle\,| = |Stab(C\,|0\rangle)| = 2^1 \implies C\,|0\rangle$ is a stabilizer state. An example of a non-stabilizer state is the first bell state $\beta_1 = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, which through computation one can find that it has the following stabilizers: $I \otimes I$, $X \otimes X$, and $Z \otimes Z$. Since there are exactly 3 stabilizers, and 3 is not a power of 2, β_1 cannot be a stabilizer state.

Corollary 2.1.3. *The computational basis state $|00\ldots0\rangle$ on n-qubits is a stabilizer state. If $|\psi\rangle$ is a Stabilizer state, then there is a Clifford unitary C such that $C\,|\phi\rangle = |\psi\rangle$, where $|\phi\rangle$ is a computational basis state.*

Proof. First we prove that $|00\dots0\rangle$ is a stabilizer state by induction, where the base case is the $|0\rangle$ state which we know is a stabilizer state from above (and $|\text{Stab}\,|0\rangle\,| = 2^1$). Now assume that $|00\dots0\rangle$ is a stabilizer state on n-qubits with $|\text{Stab}\,|00\dots0\rangle\,| = 2^k$. Let $P \in \text{Stab}\,|0\rangle$ and $Q \in \text{Stab}\,|00\dots0\rangle$, then $(P\otimes Q)\,|0\rangle\,|00\dots0\rangle = P\,|0\rangle \otimes Q\,|00\dots0\rangle = |0\rangle\,|00\dots0\rangle = |00\dots00\rangle$ (n+1 qubits). So $P\otimes Q \in \text{Stab}\,|00\dots00\rangle$, and from above arguments we know that every element in $\text{Stab}\,|00\dots00\rangle$ is of this form, thus there are 2^{k+1} elements in $\text{Stab}\,|00\dots00\rangle$, making it a stabilizer state. □

Definition 2.1.4. Let $|\psi\rangle$ be a non-zero n-qubit state. The Stabilizer nullity of $|\psi\rangle$ is $\nu(|\psi\rangle) = n - log_2|\text{Stab}\,|\psi\rangle\,|$.

Proposition 2.1.5. *Let $|\psi\rangle$ be a non-zero n-qubit state and let P be an n-qubit Pauli matrix and suppose that the probability of a $+1$ outcome when measuring P on $|\psi\rangle$ is non-zero. Then there are two alternatives for the state $|\phi\rangle$ after measurement: either $|Stab\,|\phi\rangle\,| = |Stab\,|\psi\rangle\,|$ or $|Stab\,|\phi\rangle\,| \geq 2|Stab\,|\psi\rangle\,|$, both of which satisfy $\nu(|\phi\rangle) \leq \nu(|\psi\rangle)$.*

Proof. First consider the simple case when P is in $\text{Stab}|\psi\rangle$. In this case, the "+1" measurement outcome occurs with probability 1 and $|\psi\rangle$ is unchanged. When P is not in $\text{Stab}|\psi\rangle$ we consider two alternatives. The first alternative is that P commutes with all elements of $\text{Stab}|\psi\rangle$. Recall we have the post-measurement state $|\phi\rangle = \frac{P|\psi\rangle}{\sqrt{\langle\psi|P^\dagger P|\psi\rangle}} = \frac{P|\psi\rangle}{\sqrt{\langle\psi||\psi\rangle}}$, and let $Q \in \text{Stab}\,|\psi\rangle$. Then $Q\,|\phi\rangle = \frac{QP|\psi\rangle}{\sqrt{\langle\psi||\psi\rangle}} = \frac{PQ|\psi\rangle}{\sqrt{\langle\psi||\psi\rangle}} = \frac{P|\psi\rangle}{\sqrt{\langle\psi||\psi\rangle}} = |\phi\rangle$. Note also that $\text{Stab}|\phi\rangle$ also contains $P\text{Stab}|\psi\rangle$, and thus $\text{Stab}|\phi\rangle$ contains $\text{Stab}|\psi\rangle \cup P\text{Stab}|\psi\rangle$ and thus its size is at least $2|\text{Stab}\,|\psi\rangle\,|$.

The second alternative is when P anti-commutes with some element $Q \in \text{Stab}|\psi\rangle$. Note that $Q\,|\psi\rangle = |\psi\rangle$ and $QPQ = -P$, so the probability of the $+1$ outcome is $\langle\psi|\,(I+P)\,|\psi\rangle\,/2 = \langle\psi|\,Q(I+P)Q\,|\psi\rangle\,/2 = \langle\psi|\,(I-P)\,|\psi\rangle\,/2$, which is the probability of the -1 outcome. Thus the probability of the $+1$ outcome is $1/2$. Then $|\phi\rangle = (I+P)/\sqrt{2}\,|\psi\rangle$ where we fixed the normalization condition such that $\langle\phi|\,|\phi\rangle = \langle\psi|\,|\psi\rangle$. Also, observe that we can write $|\phi\rangle = (I+PQ)/\sqrt{2}\,|\psi\rangle$. Since $(I+PQ)/\sqrt{2}$ is a Clifford unitary equal to $\exp(i\pi P'/4)$ for $P' = iPQ$, we see that $|\phi\rangle$ and $|\psi\rangle$ differ by a Clifford and therefore $|\text{Stab}|\psi\rangle\,| = |\text{Stab}|\phi\rangle\,|$. □

Definition 2.1.6 (Pauli Spectrum)**.** Let $|\psi\rangle$ be a non-zero n-qubit state. The Pauli spectrum $\text{Spec}|\psi\rangle$ of ψ is:

$$\text{Spec}\,|\psi\rangle = \left\{ \frac{|\,\langle\psi|\,P\,|\psi\rangle\,|}{\langle\psi|\psi\rangle}, \forall P \in \{I, X, Y, Z\}^{\otimes n} \right\} \tag{2.1}$$

The Pauli spectrum is a list of 4^n real numbers each between 0 and 1 which is invariant under Clifford gates. Consider the following example.

Proposition 2.1.7. *The Pauli spectrum of the state* $|\theta\rangle = (|0\rangle + e^{i\theta}|1\rangle)/\sqrt{2}$ *is* $\{1, cos\theta, sin\theta, 0\}$. *The state* $|\theta\rangle$ *is therefore a stabilizer state only for* $\theta = m\pi/2$ *for some integer* m.

Proof. First note that $|\theta\rangle$ is normalized so $\langle\theta| |\theta\rangle = 1$. Now by direct computation, we have:

- $\langle\theta| I |\theta\rangle = \langle\theta|\theta\rangle = 1$
- $\langle\theta| X |\theta\rangle = (\langle 1| e^{-i\theta} + \langle 0|)(|1\rangle + e^{i\theta}|0\rangle)/2 = (e^{-i\theta} + e^{i\theta})/2 = cos\theta$
- $\langle\theta| Y |\theta\rangle = (\langle 1| e^{-i\theta} + \langle 0|)(i|1\rangle - ie^{i\theta}|0\rangle)/2 = i(e^{-i\theta} - e^{i\theta})/2 = i(-2sin\theta)/2 = sin\theta$
- $\langle\theta| Z |\theta\rangle = (\langle 1| e^{-i\theta} + \langle 0|)(|0\rangle - e^{i\theta}|1\rangle)/2 = 1 - 1 = 0$

Moreover, if $\theta = 2k\pi/2$ for some integer k, then $X \in \mathrm{Stab}\,|\theta\rangle$, and if $\theta = (2k+1)\pi/2$, then $Y \in \mathrm{Stab}\,|\theta\rangle$. Observe that $\forall\theta$, $I \in \mathrm{Stab}\,|\theta\rangle$ and $Z \notin \mathrm{Stab}\,|\theta\rangle$, thus $|\mathrm{Stab}\,|\theta\rangle\,| = 2$ if and only if either X or $Y \in \mathrm{Stab}\,|\theta\rangle$, or more generally if $\theta = m\pi/2$, for some integer m. □

Note that the number of 1s in the Pauli spectrum of $|\psi\rangle$ is $|\mathrm{Stab}\,|\psi\rangle\,|$.

2.2 Catalysis

Theorem 2.2.1. *Let* F *be a number field which contains* $\mathbb{Q}(i)$ *and which is closed under complex conjugation. Any stabilizer circuit applied to a density matrix with all entries in* F *produces a density matrix with all entries in* F*, with both density matrices written in the computational basis.*

For example, no stabilizer circuit on any number of $|CS\rangle$ or $|CCZ\rangle$ states (which have density matrices with all entries in $\mathbb{Q}(i)$) can be used to produce a $|T\rangle$ state (which has a density matrix with all entries in $\mathbb{Q}(\zeta_8)$). Similarly, no stabilizer circuit on any number of $|T\rangle$ states can be used to produce a $|\sqrt{T}\rangle$ state (with entries in $\mathbb{Q}(\zeta_{16})$).

Proof. Suppose our stabilizer circuit acts upon N qubits initially in the $|0\rangle$ state. Clearly the density matrix $\rho_{initial} = (|0\rangle\langle 0|)^{\otimes n}$ has entries over $\mathbb{Q}$. We point out that all Clifford unitaries can be written as matrices with entries over $\mathbb{Q}(i)$, and therefore as matrices with entries over F. Explicitly, the Clifford group is generated by H, CZ, and S which are defined as:

$$H = \frac{1}{1+i}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

$$S : |0\rangle \mapsto |0\rangle, |1\rangle \mapsto |1\rangle$$

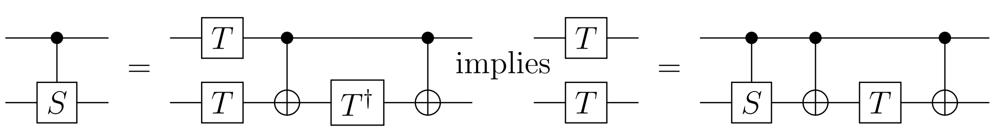
$$CZ : |ab\rangle \mapsto (-1)^{a \wedge b} |ab\rangle$$

Given any gate U in the circuit is a tensor product of a unitary with entries over F and I and ρ has entries over F the product $U\rho U^\dagger$ is a density matrix with entries over F. Therefore applying the gates in the circuit preserves the required property. Note that measurement with or without post-selection can be described as:

$$\rho \mapsto \frac{P\rho P}{Tr\rho P}$$

$$\rho \mapsto \sum_{P \in \mathcal{P}} P\rho P$$

The projectors P above correspond to measurement in the computational basis and therefore can be written as matrices with entries over $\mathbb{Q}(i)$ and therefore over F. The product of matrices over F is a matrix over F. The trace of a matrix over F is also in F by the definition of a field. The quotient of a matrix over F and an element of F is again a matrix over F because any field is closed under the division operation. This completes the proof. $\square$



Definition 2.2.2 (Conversion Notation)**.** The equation $|A\rangle \to |B\rangle$ indicates that resource state $|A\rangle$ can be converted into resource state $|B\rangle$ with stabilizer operations in the absences of a catalyst. On the other hand, $|A\rangle \xrightarrow{|C\rangle} |B\rangle$, which is equivalent to $|A\rangle |C\rangle \to |B\rangle |C\rangle$, indicates the conversion can proceed with the use of a catalyst $|C\rangle$ (which may sometimes be omitted above the arrow). When a process is impossible, we strike through the arrow, for example $|A\rangle \not\Rightarrow |B\rangle$ signifies that $|A\rangle$ cannot be converted to $|B\rangle$ by stabilizer operations even in the presence of an arbitrary catalyst. In cases involving multiple copies of a given state such as $|A\rangle^{\otimes 2} \xRightarrow{|C\rangle} |B\rangle$, we sometimes write $2|A\rangle \xRightarrow{|C\rangle} |B\rangle$ to avoid clutter.

Chapter 3

Conversion of Resource States

Theorem 3.0.1. *Let $|U\rangle$ be an n-qubit magic state for a diagonal unitary U from the 3^{rd} level of the Clifford hierarchy, and let $\tau(U)$ be the minimum number of T gates needed to implement U using the gate set $\{CNOT, S, T\}$. The following resource conversion is possible*

$$|U\rangle \xRightarrow{|T\rangle^{\otimes\tau(U)-\nu(|U\rangle}} |T\rangle^{\otimes 2\nu(|U\rangle)-\tau(U)}$$

Proof. Recall the following phase polynomial formalism. For any diagonal unitary in the 3rd level Clifford hierarchy we have $U_f = \sum_x exp(if(x)\pi/4)\,|x\rangle\langle x|$, where $f : \mathbb{Z}_2^n \to \mathbb{Z}_8$ is of cubic form and so can be decomposed as the phase polynomial $f(x) = \sum_{a_k \neq 0} a_k\lambda_k(x)$ (mod 8) where $a_k \in \mathbb{Z}_8$ and each λ_k is a $\mathbb{Z}_2$ linear function. That is, each λ_k has the form $\lambda_k(x) = (P_{1,k}x_1)\oplus(P_{2,k}, x_2)\ldots(P_{n,k}, x_n)$ (mod 2) where $P_{j,k}$ are binary. Thus we can describe the function by a binary matrix P and vector a, with columns corresponding to nonzero a_k (so the number of columns is the number of terms in f). For a function with a single term $f(x) = a_k\lambda_k(x)$, an easily verified circuit decomposition is $U_{\lambda_k} = \sum_x exp(i\lambda_k(x)\pi/4)\,|x\rangle\langle x| = V^\dagger_{CNOT(\lambda_k)}T_1^{a_k}V_{CNOT(\lambda_k)}$ where T_1 is a T gate acting on qubit 1 and $V_{CNOT(\lambda_k)}$ is a cascade of CNOT gates such that

$$V_{CNOT(\lambda_k)}\,|x\rangle = V_{CNOT(\lambda_k)}\,|x_1, x_2, \ldots x_n\rangle = |\lambda_k(x_1), x_2, \ldots x_n\rangle.$$

Now note that if a_k is even then $T_a^{a_k} = S_1^{a_k/2}$ is a Clifford and the whole circuit is Clifford. But if a_k is odd then $T_1^{a_k} = T_1S_1^{(a_k-1)/2}$ and only a single T gate is used. Now, generalizing to a phase polynomial f with many terms we have $U_f = \prod_k U_{\lambda_k}$ and so the T-count for the associated circuit is equal to the number of odd valued a_k (so if all values are even then the unitary is Clifford).

This allows us to split the unitary U_f into a Clifford and non-Clifford part. For each a_k coefficient, we define $b_k \in \mathbb{Z}_4$ and $c_k \in \mathbb{Z}_2$ such that $a_k = 2b_k + c_k$ (so $c_k = 1$ if and only if a_k is odd). Now for functions $g(x) = \sum_{c_k \neq 0} c_k\lambda_k(x)$ and $h(x) = \sum_{b_k \neq 0} b_k\lambda_k(x)$ we have that $f = g + h$ and $U_f = U_{g+2h} = U_gU_{2h}$ where U_{2h} is a Clifford Unitary. The non-Clifford part is U_g and all the terms have odd valued co-coefficients, so the number of terms in g gives an upper bound on $\tau(U_g)$ as discussed earlier. It follows that if the function g has m (odd-valued) terms then the state can be prepared using m many T gates/states. Note that for any given unitary U_g there is an equivalence class of different functions g that all result in the same unitary but with different numbers of terms. From now on we will assume that g is the optimal representative with the fewest number of terms, denoted by $\tau(U_g)$. Furthermore, there is a binary matrix P description of g with a number of columns also equal to $\tau(U_g)$. A trivial but relevant example is $U = T^{\otimes n}$ for which $P = \mathbb{1}_n$ and $\tau(T^{\otimes n}) = n$.

The next important step is that given a unitary U_g we may also be able to remove terms from g by applying inverse T gates. More generally, given two such unitaries U_g and $U_{g'}$ with phase polynomials g and g', we have that $U_{g'} = U_g U_\Delta$ where $\Delta = g - g'$. Therefore,

$$|U_{g'}\rangle = U_\Delta |U_g\rangle \tag{3.1}$$

and

$$|T\rangle^{\otimes \tau(U_\Delta)} |U_{g'}\rangle \to |U_g\rangle \tag{3.2}$$

The number of T states needed is $\tau(U_\Delta)$, which just the number of terms where g and g' differ.

Using arguments from [**?**], given any P we can always bring it into row-reduced echelon form using a CNOT circuit. Then

$$P = \begin{pmatrix} \mathbb{1}_r & A \\ 0 & 0 \end{pmatrix} \tag{3.3}$$

where $\mathbb{1}_r$ is an identity matrix of size $r := \text{rank}(P)$. If P is full rank the additional 0 padding is not present. Note that if P has any 0 rows then the unitary acts trivially on the corresponding qubits leaving them in the $|+\rangle$ state, meaning that $|U\rangle = U|+\rangle = |\psi\rangle |+\rangle^{\otimes(n-r)}$ for some state $|\psi\rangle$. Also, for an n qubit stabilizer state $|\phi\rangle$,

$$\nu(|\phi\rangle) = 0 \Rightarrow \log_2 |Stab\,|\phi\rangle\,| = n \tag{3.4}$$

Next, observe that

$$\begin{aligned}\log_2 |Stab\,|U\rangle\,| =& \log_2 |Stab(|\psi\rangle |+\rangle^{\otimes(n-r)})| \\ =& \log_2(|Stab\,|\psi\rangle\,| \cdot |Stab\,|+\rangle^{\otimes(n-r)}\,|) \\ =& \log_2 |Stab\,|\psi\rangle\,| + \log_2 |Stab\,|+\rangle^{\otimes(n-r)}\,| = \quad \log_2 |Stab\,|\psi\rangle\,| + (n-r) = \alpha + n - r\end{aligned}$$

for some positive integer $\alpha = \log_2|Stab\,|\psi\rangle\,|$. Hence $\log_2|Stab\,|U\rangle\,| \geq n - r$, so rearranging we have that $n - \log_2|Stab\,|U\rangle\,| = \nu(|U\rangle) \leq r$.

Using our earlier argument, we can always remove from P the columns corresponding to the matrix A using a number of T states equal to the number of columns in A. Since A has $\tau(U_g) - r$ columns, this requires the same quantity of T states. The resulting $U_{g'}$ has $P' = \mathbb{1}_r$ (with possibly some 0 row padding) which corresponds to r copies of T states. Therefore, we can perform

$$|U_g\rangle\,|T\rangle^{\otimes(\tau(U_g)-r)} \rightarrow |T\rangle^{\otimes r} \tag{3.5}$$

If $r = \nu(U_g)$ then we have the result of the theorem. If $r > \nu(U_g)$ then the result is even stronger than the theorem, and so the theorem holds in either case. $\square$

Chapter 4

Conclusion

Did it!