Quantum Primitives

Joseph Spring

Quantum Information & Probability Group,
School of Computer Science, University of Hertfordshire,
Hatfield, Herts AL10 9AB, UK
j.spring@herts.ac.uk

Abstract. We explore possible characterisations of entanglement classes which may be interpreted as gates acting on globally distributed systems. The cyclic nature of a selection of *entanglement gates*, primitives, is explored commencing with gates for generating Bell, GHZ and W states.

Keywords: Entanglement, Irreducibility, Prime, Separability
PACS: 02.20-a, 03.65.Fd, 03.67.Ac, 03.67.Bg, 03.67.Dd

INTRODUCTION

Cyclic Groups and Finite Fields. [1, 2, 3]. Central to classical error detection schemes such as the cyclic redundancy check, found at the link layer in network protocols such as BISYNC, HDLC, DDCMP, CSMA and token ring, is the concept of a cyclic structure operating within a finite field. These may take various forms such as $\mathbb{Z}_p$ with p prime, $p \in \mathbb{N}^+$, $\mathbb{Z}_p[x]\backslash f$ in which f is an irreducible divisor, or involve geometric constructions such as $E_p(a,b)$, in for example, elliptic and hyperelliptic settings. Related algebraic and geometric structures appear within a quantum setting in for example [4, 5, 6, 7, 8, 9, 10], whilst within a classical setting they are to be found in symmetric and asymmetric cryptography, where they play a major role. Motivated by alternative applications for cyclic structures, the role of primes and irreducibilty in both classical and quantum settings, and the similarity between entanglement and irreducibilty from an algebraic perspective, we consider properties of gates used to generate such states.

Ambient Space, Primes and Entanglement. [11]. Entanglement and primes share a common property in that their status is dependent upon the space in which they are perceived to belong. 17 = (4 + i)(4 - i) for example is prime over $\mathbb{Z}$ but not over $\mathbb{Z}(i)$, likewise $X^2 + 1$ is irreducible for $\mathbb{R}[x]$ when the roots are restricted to $\mathbb{R}$ but not over $\mathbb{C}$. Likewise, Bell states are seen to be entangled provided they are restricted to the action of operators from $\mathscr{B}(\mathscr{H}) \otimes \mathscr{B}(\mathscr{H})$ with $\mathscr{H}$ a one particle, two dimensional Hlbert space. However if we extend the operator space to $\mathscr{B}(\mathscr{H} \otimes \mathscr{H})$ then the Bell states are seen to be separable. It is the potential for global operators that characterises a state as either entangled or separable. Here we consider 'Bell gates' from $\mathscr{B}(\mathscr{H} \otimes \mathscr{H})$, $\mathscr{B}(\mathscr{H} \otimes \mathscr{H} \otimes \mathscr{H})$ and related spaces.

Bell States. Bell states are entangled states over $\mathscr{B}(\mathscr{H}) \otimes \mathscr{B}(\mathscr{H})$ and may be generated by a combination of local unitary Hadamard and Identity gates in $\mathscr{B}(\mathscr{H})$ followed by a global unitary CNOT gate in $\mathscr{B}(\mathscr{H} \otimes \mathscr{H})$.

CP1110, *Quantum Communication, Measurement and Computing (QCMC),*
The Ninth International Conference, edited by A. Lvovsky

Bell Gates. Consider the gate

$$B = CNOT.H \otimes I = \frac{1}{\sqrt{2}} \begin{bmatrix} I & I \\ X & -X \end{bmatrix} \text{ with } X \text{ and } I \text{ Pauli Operators acting on } \mathscr{H}$$

The action of the Bell gate on $x \in \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ results in each of the Bell states $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ in $\mathscr{H} \otimes \mathscr{H}$.

The gate B generates a cyclic group of order 8, with orbit:

$$\frac{1}{\sqrt{2}} \begin{bmatrix} I & I \\ X & -X \end{bmatrix}, \quad \frac{1}{2} \begin{bmatrix} I+X & I-X \\ -(I-X) & I+X \end{bmatrix}, \quad \frac{1}{\sqrt{2}} \begin{bmatrix} X & I \\ X & -I \end{bmatrix}, \quad \frac{1}{2} \begin{bmatrix} X & 0 \\ 0 & X \end{bmatrix},$$

$$\frac{1}{\sqrt{2}} \begin{bmatrix} X & X \\ I & -I \end{bmatrix}, \quad \frac{1}{2} \begin{bmatrix} I+X & -(I-X) \\ I-X & I+X \end{bmatrix}, \quad \frac{1}{\sqrt{2}} \begin{bmatrix} I & X \\ I & -X \end{bmatrix}, \quad \begin{bmatrix} I & 0 \\ 0 & I \end{bmatrix}$$

Assigning each of the given Bell states in different orders to the basis states $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ generates 4! different possible gates from B. Different orders result for the orbits of the cyclic groups generated by these gates. A self adjoint version of B, for example, such as $\frac{1}{\sqrt{2}} \begin{bmatrix} X & I \\ I & -X \end{bmatrix}$ generates a cyclic group of order 2 whilst one such as $\frac{1}{\sqrt{2}} \begin{bmatrix} I & I \\ iY & -iY \end{bmatrix}$ generates a cyclic group of order 24.

It may be shown that of the 4! possible gates suggested, 4 generate cyclic groups of order 24, 4 generate cyclic groups of order 12, 10 generate cyclic groups of order 8, 4 of order 4 and 2 of order 2. The orbits involve operators, each of whose action on $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, either result in 4 entangled states or 4 separable states. The cyclic groups generated by each of the 4! gates are likewise either gates generating separable states or gates generating entangled states. In any cyclic group generated there is found to be either 1, 2 or 4 gates whose action leads to entangled states. B for example has just 2 gates leading to entangled states, B and B^5.

Let $B_1 = \frac{1}{\sqrt{2}} \begin{bmatrix} I & I \\ -X & X \end{bmatrix}$ and $B_2 = \frac{1}{\sqrt{2}} \begin{bmatrix} X & X \\ -I & I \end{bmatrix}$ be two permutations of B. Then $B_1 = -B_2^5$. Likewise for $B_3 = \frac{1}{\sqrt{2}} \begin{bmatrix} X & X \\ I & -I \end{bmatrix}$ we find that $B = B_3^5$. It follow that the cyclic group <B> generated by gate B is identical to that generated by gate B_3, so $< B >=< B_3 >$ and $< B_1 >=< -B_2^5 >$.

Theorem The general form for the operator B generating GHZ states is

$$\frac{1}{\sqrt{2}} \begin{bmatrix} \otimes I & \otimes I \\ \otimes X & -\otimes X \end{bmatrix}$$

Proof. This follows by construction. We commence with the sum of the least binary value $|000\ldots0\rangle$ and the greatest binary value $|111\ldots1\rangle$. This gives the first entry in the

I Pauli operator and the first entry in the X Pauli operator. We then add one to the least binary value and subtract one from the greatest binary value to obtain the second column in the I operator and the second column in the X operator. Continuing in this way to the half way point in our construction generates $\otimes I$ for the upper half of the gate and $\otimes X$ for the lower half of the gate. Following this we take the 'conjugate' of the second part of the sum from the first column, then the second column, then ... column generating $\otimes I$ for the remaining upper half of the gate and -$\otimes X$ for the remaining lower half of the gate. The scalar follows by normalisation. □

The orbit for the given GHZ gate is found to be 8.

W Gates. The smallest W gate is $2^3 \times 2^3$ leading to $2^3!$ different gates that one may use to generate W states from the 2^3 basis states $\{|ijk\rangle\}$ in which $i, j, k \in \{0, 1\}$.

Definition We define a starting global gate W for describing the generation of W-states in $\mathscr{H} \otimes \mathscr{H} \otimes \mathscr{H}$ to be:

$$W = \frac{1}{\sqrt{3}} \begin{bmatrix} I & e_3 & X & e_1 \\ -e_3 & -I & e_1 & X \\ -X & e_4 & I & -e_2 \\ e_4 & -X & e_2 & -I \end{bmatrix}$$

Proposition The gate $W \in \mathscr{B}(\mathscr{H} \otimes \mathscr{H} \otimes \mathscr{H})$ is a cyclic operator of order 8.

Proof. $W^2 = \frac{1}{\sqrt{3}} \begin{bmatrix} 0 & 0 & X & 0 \\ 0 & 0 & 0 & -X \\ -X & 0 & 0 & 0 \\ 0 & X & 0 & 0 \end{bmatrix}$,

$W^4 = -I$, and $W^8 = I$.

□

A greater degree of complexity emerges in the cyclic groups generated by W gates. These range from gates generating cyclic groups of order 2, for example:

$$W_1 = \frac{1}{\sqrt{3}} \begin{bmatrix} I & |1\rangle\langle 0| & X & |0\rangle\langle 0| \\ -|1\rangle\langle 0| & -I & |0\rangle\langle 0| & X \\ -X & -|1\rangle\langle 1| & I & -|0\rangle\langle 1| \\ |1\rangle\langle 1| & -X & |0\rangle\langle 1| & -I \end{bmatrix}$$

to gates such as

$$W_2 = \frac{1}{\sqrt{3}} \begin{bmatrix} I & |1\rangle\langle 0| & X & |0\rangle\langle 1| \\ -|1\rangle\langle 0| & -I & |0\rangle\langle 0| & I \\ -X & |1\rangle\langle 1| & I & -|0\rangle\langle 0| \\ |1\rangle\langle 1| & -X & |0\rangle\langle 1| & -X \end{bmatrix}$$

.

EL-GAMAL

The generation of cyclic elements lends itself to encryption protocols such as El-Gamal, illustrating in principle, the possibility for masking the choice of gate employed at different stages within an application. Further research in this, the above and related areas has been carried out. The details will appear elsewhere.

ACKNOWLEDGMENTS

Many thanks to all those at QCMC08 for their warm hospitality and stimulating discussions.

REFERENCES

1. L. L. Peterson and B. S. Davie, *Computer Networks: A Systems Approach*, Morgan Kaufmann, Elsevier,2007.
2. Henri Cohen and Gerhard Frey (et. al.), *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, Discrete Mathematics and its Application, Chapman & Hall/CRC, 2006.
3. Joan Daemen and Vincent Rijmen, *The Design of Rijndael, AES - The Advanced Encryption Algorithm*, Springer - Verlag, 2002.
4. Stephane Beauregard, Gilles Brassard and Jose Manuel Fernandez, *Quantum Arithmetic on Galois Fields*, quant-ph 0301163, pp 1-29, 2003.
5. Kathleen S. Gibbons, Mahew J. Hoffman and William K. Wooters, *Discrete Phase Space based on Finite Fields*, quant-ph/0401155, 2004.
6. Haret Rosu, Michael Planat and Metod Saniga, *From Finite Projective Geometry to Quantum Phase Enciphering*, Quantum Communication, Measurement and Computing, edited by S. M. Barnett *et al.*, American Institute of Physics, New York, 2004.
7. Michael Planat, Haret Rosu,Serge Perrine and Metod Saniga, *Finite Algebraic geometric Structures Underlying Mutually Unbiased Quantum Measurements*, R. Buchanan et al. (es.); Time, Quantum and the Subjective;quant-ph/0503159, World Scientific Publishing Co., pp409-426, 2004.
8. Michael Planat, *Huyghens, Bohr, Riemann and Galois Phase Locking*, International Journal of Modern Physics B;quant-ph/0510044, World Scientific Publishing Co., pp 1-18, 2005.
9. Hashang Heydari, *Geometical Structure of Entangled States and Secant Variety*, quant-ph/0611144, pp 1-7, 2006.
10. J. A. Vaccaro, J. Spring and A. Chefles *Quantum Protocols for Anonymous Voting and Surveying*, Physical Review A,75, 012333, 2007.
11. Joseph Spring, *Entanglement and Irreducibilty*, Quantum Communication, Measurement and Computing 8, AIP, 2006.