

1086-22-2538

**Jennifer R. Daniel\*** ([jennifer.daniel@lamar.edu](mailto:jennifer.daniel@lamar.edu)), Department of Mathematics, Campus Box 10047, Lamar University, Beaumont, TX 77710, and **Alys M. Rodriguez**. *Using a  $(\sigma, \theta)$ -basis for the  $KAK$  decomposition in Quantum Computation.*

In quantum computation, new states evolve from initial states under a series of unitary transformations. The set of all unitary transformations form a Lie group called the unitary group  $U(2^n)$ . Without loss of generality, we only consider those unitary transformations in  $SU(2^n)$  the Lie group of unitary matrices with determinant one. Decomposing arbitrary unitary transformations into the product of simple quantum gates is crucial to understanding the design of a quantum computer. One method of such decomposition utilizes consecutive Cartan decompositions into the  $\pm 1$ -eigenspaces  $\mathfrak{k}$  and  $\mathfrak{p}$  of an involutive automorphism  $\theta$  of the Lie algebra  $\mathfrak{su}(2^n)$ . The Cartan decomposition induces a decomposition on the group level  $SU(2^n) = KAK$ , where  $H = \exp(\mathfrak{a})$  for a maximal toral subalgebra  $\mathfrak{a}$  of  $\mathfrak{p}$ . Root space decomposition is utilized as a means of establishing a basis for  $\mathfrak{k}$  and  $\mathfrak{p}$  in the  $KAK$  decomposition. Once a basis is established, we can obtain a decomposition of any  $U \in SU(2^n)$  into one qubit and controlled-not gates by exponentiating. (Received September 25, 2012)