The Quantum Entanglement of Bipolar Sequences

Matthew.G.Parker[1]
University of Bergen
Department of Informatics
Høyteknologisenteret
N-5020 Bergen, NORWAY
e-mail: matthew@ii.uib.no

V.Rijmen
Katholieke Universiteit Leuven,
Dept. Elektrotechniek-ESAT,
K. Mercierlaan 94,
B-3001 Heverlee, Belgium

Abstract — **Classification of different forms of quantum entanglement is an active area of research, central to the development of effective quantum computers, and similar to classification of error-correction codes, where the concept of code duality is broadened to equivalence under all 'local' unitary transforms. We examine links between entanglement and coding theory by forming Algebraic Normal Form (ANF) descriptions for bipolar indicator sequences to describe binary codes with codewords which occur with bipolar probabilities. Quadratic entanglement is the basis of particle-entangling arrays found in recent literature.**

I. Definition of Entanglement

Recent interest in Quantum Computation has fuelled a desire to understand Quantum Entanglement. Entanglement exists between any two or more systems if their joint probability state cannot be factorised using the tensor product. Consider two qubits, x_0 and x_1. Their joint probability state is given by,

$$\mathbf{s} = (s_0, s_1, s_2, s_3)$$

where the s_i are complex and $\sum_{i=0}^{3} |s_i|^2 = 1$. There is a probability of $|s0|^2$,$|s1|^2$,$|s2|^2$,$|s3|^2$ of measuring the two qubits in states $00, 01, 10, 11$, respectively. If $\mathbf{s}$ can be written as $(a_0, b_0) \otimes (a_1, b_1)$, then $\mathbf{s}$ is tensor-factorisable and the two qubits are not entangled. Conversely, if we cannot write $\mathbf{s}$ in the above form then the two qubits are entangled. This idea generalises in an obvious manner to m qubits. Conventional (classical) computers only ever use tensor-factorisable space of physical matter. But the existence of entanglement between quantum particles allows us to store and operate on exponentially larger data vectors than possible classically.

II. Entanglement and Error-Correction Codes

Here and in the rest of the paper normalisation of the joint-state vector is omitted for clarity. Normalisation would ensure $\sum_{i=0}^{2^n-1} |s_i|^2 = 1$. Consider the two-qubit entangled vector, $\mathbf{s} = (1, 0, 0, 1)$. Measurement of the two qubits produces states 00 and 11 with equal likelihood. 01 and 10 are never measured. We could think of $\mathbf{s}$ as the 'indicator' sequence for the parity-check $[2, 1, 2]$ code, $\mathbf{C} = \{00, 11\}$. $\mathbf{C}$ corrects errors because $\mathbf{s}$ is entangled (there is mutual information between qubits). This state is known as the 'CAT' state in physics literature. In contrast, consider the two-qubit unentangled vector, $\mathbf{s} = (1, 0, 1, 0) = (1, 0) \otimes (1, 1)$. $\mathbf{s}$ defines a $[2, 1, 1]$ code, $\mathbf{C} = \{00, 10\}$ which cannot correct errors because $\mathbf{s}$ is unentangled (there is no mutual information between qubits). Consider the three-qubit entangled vector, $\mathbf{s} = (1, 0, 0, 1, 0, 1, 1, 0)$. $\mathbf{s}$ defines a $[3, 2, 2]$ code, $\mathbf{C} = \{000, 011, 101, 110\}$ which can correct error in any of the three qubits because $\mathbf{s}$ is entangled (i.e. $\mathbf{s}$ is not tensor-factorisable).

III. Entanglement Equivalence ⇔ Code Equivalence

A unitary transform $\mathbf{U}$ satisfies $\mathbf{U}\mathbf{U}^\dagger = \mathbf{I}$ where $\dagger$ means conjugate transpose and $\mathbf{I}$ is identity. Let $\mathbf{M}$ be a $2^n \times 2^n$ unitary transform. Let $\mathbf{s}$ be the joint-state vector of n qubits.

Fact 1 *If $\mathbf{M}$ is tensor decomposable into 2×2 'local' unitaries, then the entanglement of $\mathbf{s}$ is the same as the entanglement of $\mathbf{Ms}$.*

Definition 1 *If $\exists\mathbf{M}$, where $\mathbf{M}$ is decomposable into 2×2 local unitaries, such that $\mathbf{s}' = \mathbf{Ms}$, then we write $\mathbf{s}' \equiv_{LU} \mathbf{s}$.*

Proposition 1 *If $\mathbf{s} \equiv_{LU} \mathbf{s}'$ then $\mathbf{s}$ and $\mathbf{s}'$ represent 'equivalent' error-correcting codes.*

Proposition 2 *If $\mathbf{s} \not\equiv_{LU} \mathbf{s}'$, then $\mathbf{s}$ and $\mathbf{s}'$ generally represent 'inequivalent' error-correcting codes.*

Code duality is an example of entanglement equivalence:

Proposition 3 *Let $\mathbf{C}$ be the code associated with sequence $\mathbf{s}$, and $\mathbf{C}^\perp$ be associated with $\mathbf{s}'$. Then $\mathbf{s} \equiv_{LU} \mathbf{s}'$.*

For example, $\mathbf{s}' = (1, 0, 0, 0, 0, 0, 0, 1)$ can be obtained from $\mathbf{s} = (1, 0, 0, 1, 0, 1, 1, 0)$ by application of the 8×8 Walsh-Hadamard Transform, which is tensor-decomposable. ($\mathbf{s}'$ is known amongst physicists as the GHZ state).

IV. Bipolar Entangled Sequences

We describe bipolar sequences using the Algebraic Normal Form (ANF) in the following way. Consider the bipolar sequence $+++----+$. $\log_{-1}$ of this sequence is 00011110, and the ANF for this sequence is $x_0x_1 + x_2$.

Definition 2 *'bipartite degree-m bipolar' (mB) sequences have homogeneous degree-m ANFs over 2 disjoint sets of variables, $\mathbf{L}$ and $\mathbf{R}$ such that each degree-m term in the ANF includes exactly one variable from set $\mathbf{L}$.*

For instance, bipolar sequence $+++-++-++-++-+++$ has ANF $x_0x_1 + x_1x_2 + x_2x_3 + x_3x_0$. Separating variables into two disjoint sets $\mathbf{L} = \{x_0, x_2\}$ and $\mathbf{R} = \{x_1, x_3\}$ ensures that each quadratic term in the ANF contains one variable from $\mathbf{L}$. Therefore this sequence is mB. In contrast, sequence $+++-+---+-++--+-$ has ANF $x_0x_1 + x_1x_2 + x_2x_0 + x_0x_3 + x_2x_3$. This sequence is evidently not mB.

[1]This work was funded by NFR Project Number 119390/431

Proposition 4 *mB sequences are equivalent (Proposition 1) to binary error-correcting codes. mB quadratic sequences are equivalent to* **linear** *binary error-correcting codes.*

Let $\mathbf{H} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and $\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Let '**H** acting on variable v' mean application of the tensor-decomposable transform, $\mathbf{I} \otimes \ldots \otimes \mathbf{I} \otimes \mathbf{H} \otimes \mathbf{I} \otimes \ldots \otimes \mathbf{I}$ on an n-variable indicator sequence, with $v-1$ **I**'s before the **H** and $n-v$ **I**'s after the **H**.

Proposition 5 *The mB sequence* **s** *with associated* **L** *and* **R** *sets satisfies* $\mathbf{s} \equiv_{LU} \mathbf{s}'$ *where* $\mathbf{s}'$ *is obtained from* **s** *by* **H** *acting on every variable in* **L**.

Example 1: The mB sequence $+++-++-++-++-+++++-++-++++++++-+++-+$ has ANF $x_0x_1 + x_0x_3 + x_0x_4 + x_1x_2 + x_2x_3 + x_2x_4$ and is equivalent via transform $\mathbf{I} \otimes \mathbf{H} \otimes \mathbf{I} \otimes \mathbf{H} \otimes \mathbf{H}$ to a $[5,2,2]$ binary linear error-correcting code, **C**. Alternatively it is equivalent via transform $\mathbf{H} \otimes \mathbf{I} \otimes \mathbf{H} \otimes \mathbf{I} \otimes \mathbf{I}$ to a $[5,3,2]$ binary linear error-correcting code, $\mathbf{C}^{\perp}$. We illustrate these equivalences in Fig 1 where the lh-side is the quadratic form, and the rh-side is a factor graph [2] for the binary code (the cross in a box represents parity).

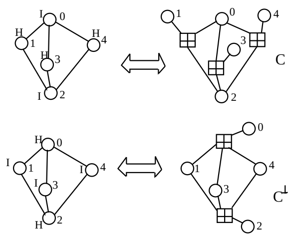


Figure 1: Bipolar to Binary Equivalence (Quadratic)

Example 2: The mB sequence $+++++++-+++-++--$ has ANF $x_0x_1x_2 + x_1x_2x_3 + x_0x_1x_3$. It is equivalent via $\mathbf{I} \otimes \mathbf{H} \otimes \mathbf{I} \otimes \mathbf{I}$ to a nonlinear $[4,3,1]$ binary code. In this example there is no other possible configuration. Fig 2 shows the equivalence where the left-hand-side is a **cubic** form, and the right-hand side is a factor graph for the binary code. The triangle in Fig 2 represents the logical operation on the rh side of Fig 2 , where the dot in a box is 'AND'.

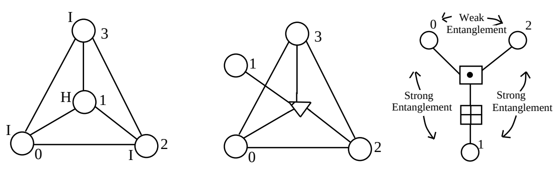


Figure 2: Binary to Bipolar Equivalence (Cubic)

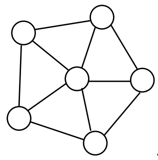
V. Entanglement Measures

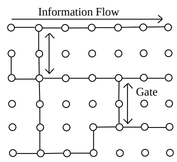
A (partial) quantification of entanglement of **s** of length 2^n (n qubits) is achieved by measuring maximum possible correlation of **s** with any 'linear' sequence **l**, where **l** is any normalised sequence of the form $\mathbf{l} = (a_0, b_0) \otimes (a_1, b_1) \otimes \ldots \otimes (a_{n-1}, b_{n-1})$. This correlation maximum can be expressed as a 'Peak-to-Average-Power-Ratio' (PAPR_l). Thus,

$$\mathrm{PAPR}_l(\mathbf{s}) = \max_{\mathbf{l}}\left(\frac{|\mathbf{s} \cdot \mathbf{l}|^2}{2^n}\right)$$

where $\cdot$ means 'inner product' [3]. **s** is completely uncorrelated with all linear sequences and wholly correlated with a particular linear sequence (unentangled) when its PAPR_l is 1 and 2^n, respectively. PAPR_l is invariant under local unitary transformation. The smaller PAPR_l, the higher the linear entanglement.

Conjecture 1 *$PAPR_l$ of a quadratic mB sequence which is equivalent to an $[n,k,d]$ binary linear code is 2^{n-r}, where $r = min(k, n-k)$.*

Conjecture 1 implies length 2^n quadratic mB sequences with high 'linear' entanglement are equivalent to length n binary linear codes with dimension $\lfloor \frac{n}{2} \rfloor$. Non-$mB$ bipolar sequences can have PAPR_l less than $2^{\lfloor \frac{n}{2} \rfloor}$. For instance, the non-$mB$ bipolar sequence with ANF $x_0x_1 + x_0x_2 + x_0x_3 + x_0x_4 + x_0x_5 + x_1x_4 + x_1x_5 + x_2x_3 + x_2x_4 + x_3x_5$ or any of its 72 variable permutations has $\mathrm{PAPR}_l = 4.0$. There are no other length 2^6 bipolar quadratics which have PAPR_l this low. Its sequence graph looks like this . PAPR_l examines multipartite 'linear' entanglement between $x_0, x_1, \ldots, x_{n-1}$. However, we also need to examine entanglement between (x_0, x_1) and $x_2, x_3, \ldots, x_{n-1}$, or (x_0, x_1, x_2) and $x_3, \ldots, x_{n-1}$, or any partition of the n variables. This is the subject of current work, where higher 'entropies of entanglement' are considered, along with classification of cubic, quartic,..etc, entanglement. Recent research [1, 4] proposed entangled arrays of particles to perform Quantum Computation like this,



They propose the entangling primitive,

$$\frac{1}{2^{N/2}} \bigotimes_{a=0}^{N-1} (|0>_a \sigma_z^{(a+1)} + |1>_a)$$

where $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. The quantum superposition is quadratic bipolar, so their arrays implement quadratic entanglement. Selective measurement then drives computation, exploiting inherent entanglement of the array.

References

[1] H.J.Briegel,R.Raussendorf, "Persistent Entanglement in Arrays of Interacting Particles," *quant-ph/0004051 v2*, 28 Aug 2000

[2] M.G.Parker, "Quantum Factor Graphs," *2nd Int. Symp. on Turbo Codes and Related Topics, Brest, France*, Long version submitted to Annals of Telecom., available on /~matthew/mattweb.html or quant-ph/0010043,Sept 4-7, 2000

[3] M.G.Parker,C.Tellambura, "Golay-Davis-Jedwab Complementary Sequences and Rudin-Shapiro Constructions," *Submitted to IEEE Trans. Inform. Theory, Preprint available on /~matthew/mattweb.html*, September 2000

[4] R.Raussendorf,H.J.Briegel, "Quantum Computing via Measurements Only", *arXiv:quant-ph/0010033*, 7 Oct 2000