S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports

http://semr.math.nsc.ru

Том 2, стр. 79–82 (2005) УДК 519.72

MSC 15A90, 94B05, 81P15

A NOTE ON CODES AND KETS

MIHAI CARAGIU

Abstract. To every binary linear $[n, k]$ code C we associate a quantum state $|\Psi_C\rangle \in H^{\otimes n}$, where H is the two-dimensional complex Hilbert space associated to the spin $\frac{1}{2}$ particle. For the state $|\Psi_C\rangle$ we completely characterize all the expectation values of the products of spins measured, for each one out of the n particles, either in the x- or in the y-direction. This establishes an interesting relationship with the dual code $C^{\perp}$.

1. INTRODUCTION

The Pauli matrices (see [4], Chapter 4) are

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

In what follows we will consider special systems of spin $\frac{1}{2}$ fermions. For a single such fermion, the Hilbert space H associated to the spin has an orthonormal basis consisting of eigenvectors of σ_z:

$$|+\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{and} \quad |-\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

In order to establish a relationship with linear codes, let us agree, for convenience, to use the following binary notation:

$$|0\rangle \ \text{ for } \ |+\rangle \quad \text{and} \quad |1\rangle \ \text{ for } \ |-\rangle.$$

Then the following matrix relations hold true:

$$\sigma_z|0\rangle = |0\rangle \ \text{ and } \ \sigma_z|1\rangle = -|1\rangle, \tag{1}$$

$$\sigma_x|0\rangle = |1\rangle \ \text{ and } \ \sigma_x|1\rangle = |0\rangle, \tag{2}$$

Caragiu M., A note on codes and kets.

Received April, 25, 2005, published June, 28, 2005 .

$$\sigma_y|0\rangle = i|1\rangle \quad \text{and} \quad \sigma_y|1\rangle = -i|0\rangle. \tag{3}$$

Let C be a linear binary $[n, k]$ code. That is C is a k-dimensional subspace of the n-dimensional vector space $\{0,1\}^n$ over the field with 2 elements. To C we associate the following quantum state (element of $H^{\otimes n}$) describing a quantum system of n spin $\frac{1}{2}$ particles:

$$|\Psi_C\rangle := \frac{1}{2^{k/2}} \sum_{(x_1,\ldots,x_n)\in C} |x_1\rangle \otimes |x_2\rangle \otimes \ldots \otimes |x_n\rangle. \tag{4}$$

Note that in the special case of the $[n, 1]$ code

$$C = \{(0,0,\ldots,0),(1,1,\ldots,1)\},$$

$|\Psi_C\rangle$ becomes the well known Green-Horne-Zeilinger (GHZ) quantum entangled state [1], [2]

$$|\Psi_{GHZ}\rangle = \frac{1}{\sqrt{2}}\left(|00\ldots0\rangle + |11\ldots1\rangle\right).$$

In what follows we will imagine that for a system of n fermions in the state $|\Psi_C\rangle$ we measure either the x-component or the y-component of the spin for each of the n particles.

To acquire a uniform binary notation we will agree to rename the operator σ_x as σ_0 and σ_y as σ_1. Also, for a bit $x \in \{0,1\}$ we will denote by $\overline{x}$ the "flipped"bit $1+x \pmod 2$. A particular measurement of x- or y- spins for the particles in (4) can be represented as a product operator of the form

$$\sigma_A = \sigma_{a_1} \otimes \ldots \otimes \sigma_{a_n},$$

where $A := (a_1,\ldots,a_n) \in \{0,1\}^n$ indicates the measurement choice we make for every particle. For example, if $n = 3$ and $A = (1,0,1)$ we measure the x-component of the spin for the second particle and the y-components of the spin for the first and the third particles. Thus, every such binary vector A codifies a selection of x- and y- spins to be measured.

It is not difficult to see that a unified binary representation of the relations (2) and (3) is given by the following:

$$\sigma_a|b\rangle = e^{i\left(\frac{\pi a}{2}+\pi ab\right)}|\overline{b}\rangle, \tag{5}$$

where a, b are bits.

The author wishes to thank the anonymous referee for the helpful comments

2. CODE DUALITY AND EXPECTATION VALUES FOR PRODUCTS OF SPINS

We will now determine the expectation value, in the quantum state $|\Psi_C\rangle$, of the product $\Pi(C, A)$ of spins codified as shown above by a certain binary vector A. For the mathematical formalism of quantum mechanics see [4], Chapter 2. In other words, we will determine

$$\Pi(C,A) = \langle\Psi_C|\sigma_A|\Psi_C\rangle$$

By using (5), we will get:

$$\sigma_A|\Psi_C\rangle = \frac{1}{2^{k/2}} \sum_{X=(x_1,\ldots,x_n)\in C} |\sigma_{a_1}x_1\rangle \otimes \ldots \otimes |\sigma_{a_n}x_n\rangle =$$

$$= \frac{1}{2^{k/2}} \sum_{X \in C} e^{\frac{i\pi}{2}(a_1 + ... + a_n) + i\pi(a_1 x_1 + ... + a_n x_n)} |\overline{x_1}\rangle \otimes ... \otimes |\overline{x_n}\rangle.$$

That is,

$$\sigma_A |\Psi_C\rangle = \frac{e^{\frac{i\pi}{2} wt(A)}}{2^{k/2}} \sum_{X \in C} e^{i\pi (A|X)} |\overline{X}\rangle, \tag{6}$$

where $wt(A)$ is the Hamming weight of the binary vector A,

$$(A|X) = a_1 x_1 + ... + a_n x_n \pmod 2$$

is the binary dot product, and

$$|\overline{X}\rangle = |\overline{x_1}\rangle \otimes ... \otimes |\overline{x_n}\rangle.$$

The following technical lemma will be essential in the derivation of our main result:

Lemma 1. *If A is a binary vector of length n and if C is a binary $[n, k]$ code, then*

$$\Pi(C, A) = \frac{e^{\frac{i\pi}{2} wt(A)}}{2^k} \sum_{X, Y \in C} e^{i\pi (A|X)} \langle Y|\overline{X}\rangle. \tag{7}$$

Proof. Indeed, (7) is a straightforward consequence of (4) together with (6) and the fact that $\Pi(C, A) = \langle \Psi_C|\sigma_A|\Psi_C\rangle$.

Two observations are in order at this point. First, note that the kets $|X\rangle$ form an orthonormal basis in the 2^n-dimensional Hilbert space $H^{\otimes n}$. Second, note that $\overline{X}$ equals $\mathbf{1} + X$ where $\mathbf{1} = (1, 1, ..., 1) \in \{0, 1\}^n$. This, together with the above lemma shows that if $\mathbf{1} \notin C$, then

$$\Pi(C, A) = \langle \Psi_C|\sigma_A|\Psi_C\rangle = 0.$$

Indeed, if $\mathbf{1} \notin C$, since C is a linear code, $\overline{C} = \{\mathbf{1} + X | X \in C\}$ is a coset of C disjoint from C so that all the products $\langle Y|\overline{X}\rangle$ in (7) will be zero.

Consider now the case $\mathbf{1} \in C$. That is, *all codewords in the dual code $C^\perp$ have even weight* (for information on linear codes and duality, see [3], Chapter 3). In this case, $\Pi(C, A)$ expressed in (7) will become

$$\Pi(C, A) = \frac{e^{\frac{i\pi}{2} wt(A)}}{2^k} \sum_{X \in C} e^{i\pi (A|\overline{X})} = \frac{e^{\frac{i\pi}{2} wt(A)}}{2^k} \sum_{X \in C} e^{i\pi (A|\mathbf{1}+X)},$$

or, keeping in mind that $(A|\mathbf{1}) = wt(A)$,

$$\Pi(C, A) = \frac{e^{\frac{i\pi}{2} wt(A)}}{2^k} e^{i\pi wt(A)} \sum_{X \in C} e^{i\pi (A|X)}. \tag{8}$$

Note that the sum appearing in (8) is zero if $A \notin C^\perp$ and 2^k if $A \in C^\perp$. Also, note that if $\mathbf{1} \in C$, then any binary vector $A \in C^\perp$ satisfies $e^{i\pi wt(A)} = 1$ since A has even weight. These observations, together with (8) show that if $\mathbf{1} \in C$ and if $A \notin C^\perp$ then

$$\Pi(C, A) = \langle \Psi_C|\sigma_A|\Psi_C\rangle = 0,$$

and that if $\mathbf{1} \in C$ and if $A \in C^\perp$ then

$$\Pi(C, A) = \langle \Psi_C|\sigma_A|\Psi_C\rangle = e^{\frac{i\pi}{2} wt(A)}.$$

Note that if $\mathbf{1} \in C$ and if $A \in C^{\perp}$, then A has even weight and therefore $e^{\frac{i\pi}{2} wt(A)} = \pm 1$, that is, $e^{\frac{i\pi}{2} wt(A)}$ is 1 if $wt(A) \equiv 0 \pmod 4$ and -1 if $wt(A) \equiv 2 \pmod 4$. This entanglement effect appears precisely when $|\Psi_C\rangle$ has nonzero components along both "GHZ kets"$|00...0\rangle$ and $|11...1\rangle$.

The next theorem brings together all the results we got in this section, completely characterizing the values of $\Pi(C, A) = \langle \Psi_C | \sigma_A | \Psi_C \rangle$.

Theorem 2. *If A is a binary vector of length n and if C is a binary $[n, k]$ code, then the following hold true:*

$\Pi(C, A) = 0$ if $\mathbf{1} \notin C$,
$\Pi(C, A) = 0$ if $\mathbf{1} \in C$ *and* $A \notin C^{\perp}$,
$\Pi(C, A) = 1$ if $\mathbf{1} \in C$, $A \in C^{\perp}$ and $wt(A) \equiv 0 \pmod 4$,
$\Pi(C, A) = -1$ if $\mathbf{1} \in C$, $A \in C^{\perp}$ and $wt(A) \equiv 2 \pmod 4$.

References

[1] D.M. Greenberger, M. Horne and A. Zeilinger, in *Bell's Theorem, Quantum Theory and Conceptions of the Universe*, M. Kafatos (editor), Kluwer Academic, Dordrecht, 1989.
[2] D.M. Greenberger, M.A. Horne, A. Shimony and A. Zeilinger, *Bell's theorem without inequalities, Amer. J. Phys.* 58 (1990), 1131-1143.
[3] J. H. van Lint, *Introduction to Coding Theory*, Third Edition, Springer Verlag, 1999.
[4] C. Cohen-Tannoudji, B. Diu and F. Laloe, *Quantum Mechanics* (Volume I), Wiley-Interscience, 1996.

Mihai Caragiu
Department of Mathematics,
Ohio Northern University
Ada, OH 45810, USA
E-mail address: m-caragiu1@onu.edu