on periodic sequences. In particular, for case i), note that the condition is violated because for any $d \geq 1$, the shift space $\mathcal{S}(d, 2d)$ contains a sequence of period $d+1$, namely, the sequence $(0^d1)^\infty = \cdots 0^d 1 0^d 1 0^d 1 \ldots$, while $\mathcal{S}(d+1, 3d+1)$ does not contain any sequence of period $d+1$ or less. The periodic sequence condition is violated in case ii) as well, since $\mathcal{S}(d, \infty)$ contains the all-zeros sequence 0^∞, which is periodic with period 1, while $\mathcal{S}(d-1, 2d-1)$, $d > 1$, does not contain the all-zeros sequence or the all-ones sequence, which are the only sequences of period 1. We would like to remark that when $d = 1$, the shift space $\mathcal{S}(d-1, 2d-1)$ does in fact contain the all-ones sequence.

The condition on periodic sequences is not strong enough to handle case iii), since $\mathcal{S}(4, \infty)$ contains the period-1 sequence consisting of all zeros. Instead, we show that there cannot exist a rate 1:1 sliding-block decodable encoder from $\mathcal{S}(4, \infty)$ to either $\mathcal{S}(1, 2)$ or $\mathcal{S}(2, 4)$ by appealing to the characteristic polynomial condition. From (3), we see that

$$\chi_{4,\infty}(z) = z^5 - z^4 - 1$$

and from (2) we find that

$$\chi_{1,2}(z) = z^3 - z - 1$$

and

$$\chi_{2,4}(z) = z^5 - z^2 - z - 1.$$

By inspection, it follows that $\chi_{4,\infty}(z)$ is not a divisor of either $\chi_{1,2}(z)$ or $\chi_{2,4}(z)$ in the ring of integer polynomials. Therefore, there does not exist a sliding-block mapping from either $\mathcal{S}(1, 2)$ or $\mathcal{S}(2, 4)$ onto $\mathcal{S}(4, \infty)$. This completes the proof of Theorem I.1.

We would like to make one final observation regarding the (d, k)-constrained shift spaces $\mathcal{S}(d, k)$. Our proof of Theorem I.1 in fact shows that given distinct shift spaces $\mathcal{S}(d, k)$ and $\mathcal{S}(\hat{d}, \hat{k})$ of equal capacity, there exists a sliding-block map from $S(\hat{d}, \hat{k})$ onto $S(d, k)$ if and only if one of Conditions 1–4 in the statement of the theorem holds. It follows that the only case where there exists a sliding-block map from $\mathcal{S}(\hat{d}, \hat{k})$ onto $\mathcal{S}(d, k)$, and from $\mathcal{S}(d, k)$ onto $\mathcal{S}(\hat{d}, \hat{k})$ as well, is when $\{(d, k), (\hat{d}, \hat{k})\} = \{(0, 1), (1, \infty)\}$. Therefore, aside from $\mathcal{S}(0, 1)$ and $\mathcal{S}(1, \infty)$, no pair of distinct (d, k)-constrained shift spaces can be conjugate. It is a well-known and trivial fact that $\mathcal{S}(0, 1)$ and $\mathcal{S}(1, \infty)$ are indeed conjugate as shift spaces, the required conjugacy being obtained by mapping 0's and 1's to their respective complements. Thus, the only pair of (d, k)-constrained shift spaces that are conjugate are $\mathcal{S}(0, 1)$ and $\mathcal{S}(1, \infty)$.

Acknowledgment

The authors wish to thank Brian Marcus for an especially thorough review of the correspondence, and for suggesting various changes to the presentation in the interests of simplicity and correctness.

References

[1] B. H. Marcus, R. M. Roth, and P. H. Siegel, "Constrained systems and coding for recording channels," in *Handbook of Coding Theory*, R. Brualdi, C. Huffman, and V. Pless, Eds. Amsterdam, The Netherlands: Elsevier, 1998.

[2] D. Lind and B. Marcus, *An Introduction to Symbolic Dynamics and Coding*. Cambridge, U.K.: Cambridge Univ. Press, 1995.

[3] K. A. S. Immink, P. H. Siegel, and J. K. Wolf, "Codes for digital recorders," *IEEE Trans. Inform. Theory*, vol. 44, pp. 2260–2299, Oct. 1998.

[4] J. Ashley, "Resolving factor maps for shifts of finite type with equal entropy," *Ergod. Theory Dynam. Syst.*, vol. 11, pp. 219–240, 1991.

[5] N. Kashyap and P. H. Siegel, "Capacity equalities in 1-dimensional (d, k)-constrained systems," in *Proc. IEEE Int. Symp. Information Theory*, Yokohama, Japan, June/July 2003, p. 105.

[6] ——, "Equalities among capacities of (d, k)-constrained systems," *SIAM J. Discr. Math.*, vol. 17, no. 2, pp. 276–297, 2003.

Binary Construction of Quantum Codes of Minimum Distance Three and Four

Ruihu Li and Xueliang Li

***Abstract*—We give elementary recursive constructions of binary self-orthogonal codes with dual distance four for all even lengths $n \geq 12$ and $n = 8$. Consequently, good quantum codes of minimum distance three and four for such length n are obtained via Steane's construction and the CSS construction. Previously, such quantum codes were explicitly constructed only for a sparse set of lengths. Almost all of our quantum codes of minimum distance three are optimal or near optimal, and some of our minimum-distance four quantum codes are better than or comparable with those known before.**

***Index Terms*—Binary code, quantum error correcting code, self-orthogonal code.**

I. Introduction

Since the initial discovery of quantum error-correcting codes [8], researchers have made great progress in developing quantum codes. Many code constructions are given in [2], [8], [9], [11]. Reference [2] gives a thorough discussion of the principles of quantum coding theory, many example codes, and a tabulation of codes and bounds on the minimum distance for codeword length n up to 30 quantum bits. For larger n there has been less progress, and only a few general code constructions are known, see [1], [2], [4], [5], [10], [11].

In [2, Theorems 10 and 11], Calderbank *et al.* proved that when n is a power of 2 or sums of odd power of 2, there exists a quantum code with parameters $[[n, n-m-2, 3]]$ for certain m, see Theorem 1.2 below. An $[[n, k, d]]$ code is an additive minimum-distance d quantum code of length n encoding k quantum bits [2]. In this correspondence, we use elementary recursive constructions to generalize their result to all even $n \geq 12$ and $n = 8$. Our quantum codes are *additive* and *pure* in the nomenclature of [2], [11]. A pure additive code is *nondegenerate* in the nomenclature of [2], [6]. Using the sphere-packing bound, we show that almost all of our quantum codes of minimum distance three are optimal or near optimal, and some of our quantum codes of minimum distance four are better than or comparable to previously known codes in [1], [2], [5], [11].

Manuscript received May 1, 2003; revised August 16, 2003.

R. Li is with the Department of Applied Mathematics and Physics, College of Art and Science, Air Force Engineering University, Xi'an, Shaanxi 710051, China, and the Department of Computer Science and Engineering, Northwestern Polytechnical University, Xi'an, Shaanxi 710016, China (e-mail: liruihu@yahoo.com.cn).

X. Li is with the Center for Combinatorics, Nankai University, Tianjin 300071, China (e-mail: x.li@eyou.com).

Communicated by E. H. Knill, Associate Editor for Quantum Information Theory.

Digital Object Identifier 10.1109/TIT.2004.828149

First, we give some notations and recall some results of [2], [3], [8], [9], [11]. In the following, we always assume that n is even and $n \geq 12$ or $n = 8, k \geq 3$, and that all the matrices and classical codes are binary.

Let H be a k by n matrix of rank k, and $\mathcal{C} = \langle H \rangle$ be the linear code generated by H. Then the *dual code* $\mathcal{C}^{\perp}$ of $\mathcal{C}$ is defined as

$$\mathcal{C}^{\perp} = \{x \in F_2^n \mid Hx^T = \mathbf{0}\}.$$

A code $\mathcal{C}$ is *self-orthogonal* if $\mathcal{C} \subseteq \mathcal{C}^{\perp}$, and *self-dual* if $\mathcal{C} = \mathcal{C}^{\perp}$. Let $\mathbf{1}_n = (1, 1, \ldots, 1)_{1\times n}$ be the all-ones vector of length n and $\mathbf{0}_t = (0, 0, \ldots, 0)_{1\times t}$ for $t \geq 1$, and let the code $\mathcal{C}_{n0} = \langle \mathbf{1}_n \rangle$. Then $\mathcal{C}_{n0}$ is self-orthogonal and $\mathcal{C}_{n0}^{\perp}$ is an $[n, n-1, 2]$ code with all words having even weight.

Theorem 1.1: Let $\mathcal{C}$ and $\mathcal{C}'$ be binary $[n, k, d]$ and $[n, k_1, d_1]$ codes, respectively.

1) **(CSS construction [3], [8], [9])** If $\mathcal{C}^{\perp} \subseteq \mathcal{C}'$, then an

$$[[n, k + k_1 - n, \min\{d, d_1\}]]$$

code can be constructed. Especially, if $\mathcal{C}^{\perp} \subset \mathcal{C}$, then there exists an $[[n, 2k - n, d]]$ code.

2) **(Steane's construction [11])** If $\mathcal{C}^{\perp} \subset \mathcal{C} \subset \mathcal{C}'$, and $k_1 \geq k + 2$, then an

$$\left[\left[n, k + k_1 - n, \min\left\{d, \left\lceil \frac{3}{2} d_1 \right\rceil\right\}\right]\right]$$

code can be constructed.

Theorem 1.2:

1) **([2, Theorem 10])** For $m \geq 3$, there exists a $[[2^m, 2^m - m - 2, 3]]$ code.

2) **([2, Theorem 11])** For odd $m \geq 3$,there exists an $[[n, n - m - 2, 3]]$ code, where

$$n = \sum_{1 \leq i \leq \frac{(m-1)}{2}} 2^{2i+1}.$$

According to the sphere-packing bound given in [2], [6], we give a reasonable definition and an obvious proposition in the following, so that in Section III, we can evaluate the optimality of the quantum codes we obtain.

Definition 1.1:

1) A nondegenerate $[[n, n-s, 2t+1]]$ code is *optimal* if there do not exist nondegenerate $[[n, n-s+1, 2t+1]]$ and $[[n, n-s, 2t+3]]$ codes.

2) A nondegenerate $[[n, n-s, 2t+1]]$ code is *near optimal* if there do not exist nondegenerate $[[n, n-s+2, 2t+1]]$ and $[[n, n-s, 2t+3]]$ codes.

Proposition 1.1:

1) If $2^{s-1} < 1 + 3n \leq 2^s < 1 + 3n + \frac{9n(n-1)}{2}$, then a nondegenerate $[[n, n-s, 3]]$ code is optimal.

2) If $2^{s-2} < 1 + 3n \leq 2^s < 1 + 3n + \frac{9n(n-1)}{2}$, then a nondegenerate $[[n, n-s, 3]]$ code is near optimal.

Our goal is to construct a code $\mathcal{C}_n = \langle H_n \rangle$ with $\mathcal{C}_{n0} \subset \mathcal{C}_n \subset \mathcal{C}_n^{\perp} \subset \mathcal{C}_{n0}^{\perp}$ and $\mathcal{C}_n^{\perp}$ an $[n, n-t, 4]$ code for some $t \leq \lceil \log_2(n+18) \rceil + 1$. According to Theorems 1.1 and 1.2, one can obtain quantum codes with parameters $[[n, n-t-1, 3]]$ and $[[n, n-2t, 4]]$. Our constructions are based on the following easily proved lemma.

Lemma 1.1: Let H_n be a k by n matrix of rank k such that

$$H_n = \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ \alpha_0 & \alpha_1 & \cdots & \alpha_{n-2} & \alpha_{n-1} \end{pmatrix} = \begin{pmatrix} & & \mathbf{1}_n & & \\ \alpha_0 & \alpha_1 & \cdots & \alpha_{n-2} & \alpha_{n-1} \end{pmatrix}.$$

If $H_n H_n^T = 0$, and the $k-1$-dimensional column vectors $\alpha_0, \alpha_1, \ldots, \alpha_{n-2}, \alpha_{n-1}$ are all different, then $\mathcal{C}_n = \langle H_n \rangle$ is self-orthogonal and $\mathcal{C}_n^{\perp}$ is an $[n, n-k, 4]$ code, and $\mathcal{C}_{n0} \subset \mathcal{C}_n \subset \mathcal{C}_n^{\perp} \subset \mathcal{C}_{n0}^{\perp}$.

II. Codes Construction

Let $k \geq 3$ be integer, for each i satisfying $0 \leq i < 2^k$, i has a representation in the base 2 as

$$i = a_0 + a_1 \times 2 + \cdots + a_{k-1} \times 2^{k-1}$$

where $a_j \in F_2$ for $0 \leq j \leq k-1$. We define

$$\varphi_k(i) = (a_0, a_1, \ldots, a_{k-1})^T \in F_2^k.$$

It is obvious that $\varphi_k(i) \neq \varphi_k(j)$ while $0 \leq i < j < 2^k$, and $\varphi_{k+t}(i) = (\varphi_k(i)^T, 0_t)^T$ for $0 \leq i < 2^k$ and $t \geq 1$.

Case A: $n = 8m, m \geq 1$.

Subcase A.1): For $m = 1$, let $\varphi = \varphi_3$, and

$$H_8 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \varphi(0) & \varphi(1) & \varphi(2) & \varphi(3) & \varphi(4) & \varphi(5) & \varphi(6) & \varphi(7) \end{pmatrix} = \begin{pmatrix} \mathbf{1}_8 \\ x_0 \\ x_1 \\ x_2 \end{pmatrix}.$$

It is well known that $\mathcal{C}_8 = \langle H_8 \rangle$ is a self-dual $[8, 4, 4]$ code.

Subcase A.2): For $m \geq 2$, let $2^{k-1} < 8m \leq 2^k$, then $2^{k-1} \leq 8(m-1) < 2^k$; so we can assume $8(m-1) = 2^{j_1} + 2^{j_2} + \cdots + 2^{k-1}$, with $j_1 < j_2 < \cdots < k-1$. We denote $I_{8(m-1)} = \{j_1, j_2, \ldots, k-1\}$, and let $\varphi = \varphi_k$. For $1 \leq s \leq m$, we define the expression at the bottom of the page. Then

$$y_j = \begin{cases} x_j, & \text{for } 0 \leq j \leq 2 \\ \mathbf{1}_8, & \text{for } j > 2 \text{ and } j \in I_{8(s-1)} \\ \mathbf{0}, & \text{for } j > 2 \text{ and } j \notin I_{8(s-1)}. \end{cases}$$

Thus, we have $H_k(8s-8, 8s-1) H_k^T(8s-8, 8s-1) = \mathbf{0}$, so we can construct a $k+1$ by n matrix $H_n = H_{8m}$ as shown in the expression at the bottom of the next page. It is obvious that the rank of H_n is $k+1$, and $H_n H_n^T = \mathbf{0}$. Thus, we have shown that $\mathcal{C}_n = \langle H_n \rangle$ satisfies

$$H_k(8s-8, 8s-1) = (\varphi(8s-8) \quad \varphi(8s-7) \quad \varphi(8s-6) \quad \varphi(8s-5) \quad \varphi(8s-4) \quad \varphi(8s-3) \quad \varphi(8s-2) \quad \varphi(8s-1)) = \begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ \vdots \\ y_{k-1} \end{pmatrix}.$$

Lemma 1.1 and $\mathcal{C}_n^\perp$ is an $[n, n - \lceil \log_2 n \rceil - 1, 4]$ code. We have now proved the following theorem.

Theorem 2.1: For $n = 8m$, $m \ge 1$, there exist codes with parameters $[[n, n - \lceil \log_2 n \rceil - 2, 3]]$ and $[[n, n - 2\lceil \log_2 n \rceil - 2, 4]]$.

Case B: $n = 8m + 2$, $m \ge 2$.

Subcase B.1): For $2 \le m \le 6$, let $\varphi = \varphi_6$ and construct H_{14}, G_1, G_2, G_3, G_4 as shown at the bottom of the following page. It is easy to check that $H_{14}H_{14}^T = \mathbf{0}$ and $G_iG_i^T = \mathbf{0}, 1 \le i \le 4$: the columns of H_{14} and G_i $(1 \le i \le 4)$ are all different, and H_{14} , G_1, G_2, G_3, and G_4 are submatrices of H_{64}. According to **CASE A**, we can construct $H_{50}, H_{42}, H_{34}, H_{26}$, and H_{18} satisfying Lemma 1.1 as follows. Delete the columns of H_{14} from H_{64} and denote the resulting matrix as H_{50}. For $1 \le i \le 4$, delete the columns of G_i from $H_{50-8(i-1)}$ and denote the resulting matrix as H_{50-8i}, thus, we can obtain H_{42}, H_{34}, H_{26}, and H_{18}.

It is easy to check that for $n = 18, 26, 34, 42, 50$, the code $\mathcal{C}_n = \langle H_n \rangle$ is self-orthogonal and $\mathcal{C}_n^\perp$ is an $[n, n - 7, 4]$ code, thus, we can obtain codes with parameters $[[n, n - 8, 3]]$ and $[[n, n - 14, 4]]$.

Subcase B.2): For $m > 6$, $n = 8m+2$. Let $2^{k-1} < 8(m+2) \le 2^k$, and let $\varphi = \varphi_k$. Construct $H_{14}(m)$ as shown at the bottom of the second next page. According to **CASE A** and the preceding discussion, delete the columns of $H_{14}(m)$ from $H_{8(m+2)}$ and denote the resulting matrix as H_n. It is easy to check that $\mathcal{C}_n = \langle H_n \rangle$ is self-orthogonal and $\mathcal{C}_n^\perp$ is an $[n, n - \lceil \log_2(n + 14) \rceil - 1, 4]$ code, thus, we can obtain codes with parameters $[[n, n - \lceil \log_2(n + 14) \rceil - 2, 3]]$ and $[[n, n - 2\lceil \log_2(n + 14) \rceil - 2, 4]]$. Thus, we have proved the following theorem.

Theorem 2.2: Let $n = 8m + 2$, $m \ge 2$.

1) If $2 \le m \le 6$, there exist codes with parameters $[[n, n - 8, 3]]$ and $[[n, n - 14, 4]]$.
2) If $m > 6$, there exist codes with parameters $[[n, n - \lceil \log_2(n + 14) \rceil - 2, 3]]$ and $[[n, n - 2\lceil \log_2(n + 14) \rceil - 2, 4]]$.

Case C: $n = 8m + 4$, $m \ge 1$.

Subcase C.1): For $m \le 2$, let $\varphi = \varphi_5$ and construct the second matrix on the bottom of the second next page. It is easy to check that the rank of H_{12} is 6 and $H_{12}H_{12}^T = \mathbf{0}$. Since H_{12} is a submatrix of H_{32}, delete the columns of H_{12} from H_{32} and denote the resulting matrix as H_{20}. According to **CASE A**, we have shown that for $n = 8m+4, m \le 2$, the code $\mathcal{C}_n = \langle H_n \rangle$ satisfies Lemma 1.1 and $\mathcal{C}_n^\perp$ is an $[n, n - 6, 4]$ code. Thus we can obtain codes with parameters $[[n, n - 7, 3]]$ and $[[n, n - 12, 4]]$.

Subcase C.2): For $m > 2$, let $2^{k-1} < 8(m + 2) \le 2^k$, and let $\varphi = \varphi_k$. Construct $H_{12}(m)$ as shown in the third matrix at the bottom of the second next page. According to **CASE A** and the preceding discussion, we delete the columns of $H_{12}(m)$ from $H_{8(m+2)}$ and denote the resulting matrix as H_n. It is easy to check that the code $\mathcal{C}_n = \langle H_n \rangle$ is self-orthogonal and $\mathcal{C}_n^\perp$ is an $[n, n - \lceil \log_2(n + 12) \rceil - 1, 4]$ code. Thus, we can obtain codes with parameters $[[n, n - \lceil \log_2(n + 12) \rceil - 2, 3]]$ and $[[n, n - 2\lceil \log_2(n + 12) \rceil - 2, 4]]$. Summarizing the above, we have proved the following theorem.

Theorem 2.3: Let $n = 8m + 4$, $m \ge 1$.

1) If $m \le 2$, there exist codes with parameters $[[n, n - 7, 3]]$ and $[[n, n - 12, 4]]$.
2) If $m > 2$, there exist codes with parameters $[[n, n - \lceil \log_2(n + 12) \rceil - 2, 3]]$ and $[[n, n - 2\lceil \log_2(n + 12) \rceil - 2, 4]]$.

Case D: $n = 8m + 6$, $m \ge 1$.

Subcase D.1): For $m \le 5$, using the matrices H_{14}, G_1, G_2, G_3, G_4 constructed in **CASE B**, we can construct H_{22}, H_{30}, H_{38}, and H_{46} satisfying Lemma 1.1 as follows:

$$H_{14+8(i-1)} = (\, H_{14+8(i-1)} \quad G_i \,).$$

Thus, for $n = 8m + 6$, $1 \le m \le 5$, the code $\mathcal{C}_n = \langle H_n \rangle$ is self-orthogonal and $\mathcal{C}_n^\perp$ is an $[n, n - 7, 4]$ code , and we can obtain codes with parameters $[[n, n - 8, 3]]$ and $[[n, n - 14, 4]]$.

Subcase D.2): For $m > 5, n = 8m+6$. Let $2^{k-1} < 8(m+3) \le 2^k$, and let $\varphi = \varphi_k$. Construct $H_{18}(m)$ as follows:

$$H_{18}(m) = \begin{pmatrix} H_{18} \\ \mathbf{0}_{(k-6)\times 18} \end{pmatrix}.$$

According to **CASE A**, **CASE B**, and the preceding discussion, delete the columns of $H_{18}(m)$ from $H_{8(m+3)}$ and denote the resulting matrix as H_n. It is easy to check that $\mathcal{C}_n = \langle H_n \rangle$ is self-orthogonal and $\mathcal{C}_n^\perp$ is an $[n, n - \lceil \log_2(n + 18) \rceil - 1, 4]$ code, thus, we can obtain codes with parameters $[[n, n - \lceil \log_2(n + 18) \rceil - 2, 3]]$ and $[[n, n - 2\lceil \log_2(n + 18) \rceil - 2, 4]]$. Summarizing the preceding discussion, we have proved the following theorem.

Theorem 2.4: Let $n = 8m + 6$, $m \ge 1$.

1) If $m \le 5$, there exist codes with parameters $[[n, n - 8, 3]]$ and $[[n, n - 14, 4]]$.
2) If $m > 5$, there exist codes with parameters $[[n, n - \lceil \log_2(n + 18) \rceil - 2, 3]]$ and $[[n, n - 2\lceil \log_2(n + 18) \rceil - 2, 4]]$.

The four cases discussed above are summarized by our main theorem as follows.

Theorem 2.5:

1) For $n > 32$, let $k \ge 6$. If $2^{k-1} < n \le 2^k - 12$, or $n = 2^k - 8$, or $n = 2^k$, there are codes with parameters $[[n, n - \lceil \log_2 n \rceil - 2, 3]]$ and $[[n, n - 2\lceil \log_2 n \rceil - 2, 4]]$.

   If $n = 2^k - a$, where $a \in \{2, 4, 6, 10\}$, there are codes with parameters $[[n, n - \lceil \log_2 n \rceil - 3, 3]]$ and $[[n, n - 2\lceil \log_2 n \rceil - 4, 4]]$.

$$\begin{aligned}
H_{8m} &= \begin{pmatrix} \multicolumn{5}{c}{\mathbf{1}_n} \\ H_k(0,7) & H_k(8,15) & \cdots & H_k(8m-16, 8s-9) & H_k(8m-8, 8m-1) \end{pmatrix} \\
&= \begin{pmatrix}
\mathbf{1}_8 & \mathbf{1}_8 & \cdots & \mathbf{1}_{2^{k-1}-2^{k-2}} & \mathbf{1}_{n-2^{k-1}} \\
x_0 & x_0 & \cdots & \cdots & \cdots \\
x_1 & x_1 & \cdots & \cdots & \cdots \\
x_2 & x_2 & \cdots & \cdots & \cdots \\
 & \mathbf{1}_8 & \cdots & \cdots & \cdots \\
 & & \ddots & \cdots & \cdots \\
 & & & \mathbf{1}_{2^{k-1}-2^{k-2}} & \cdots \\
 & & & & \mathbf{1}_{n-2^{k-1}}
\end{pmatrix} \\
&= \begin{pmatrix} \multicolumn{5}{c}{\mathbf{1}_n} \\ \varphi(0) & \varphi(1) & \cdots & \varphi(8m-2) & \varphi(8m-1) \end{pmatrix}.
\end{aligned}$$

2) For $n \leq 32$. There are codes with parameters

$$[[8,3,3]], [[8,0,4]], [[12,5,3]], [[12,0,4]],$$
$$[[14,6,3]], [[14,0,4]], [[16,10,3]], [[16,6,4]],$$
$$[[18,10,3]], [[18,4,4]], [[20,13,3]], [[20,8,4]],$$
$$[[22,14,3]], [[22,8,4]], [[24,17,3]], [[24,12,4]],$$
$$[[26,18,3]], [[26,12,4]], [[28,20,3]], [[28,14,4]],$$
$$[[30,22,3]], [[30,16,4]], [[32,25,3]], [[32,20,4]].$$

Remark: While revising this correspondence, we found that the codes $\mathcal{C}_{12}$ and $\mathcal{C}_{14}$ were called $\mathcal{B}_{12}$ and $\mathcal{D}_{14}$ in [12], respectively.

III. Concluding Remarks

In the sense of Definition 1.1, almost all of our quantum codes of minimal distance three except the $[[14,6,3]]$ code are optimal or near optimal. Using the results of [2] for $n \leq 30$, one can easily check the following result by using of Proposition 1.1.

Theorem 3.1:

1) For $n > 32$, let $k \geq 6$. If $\frac{2^{k+1}-1}{3} < n \leq 2^k - 12$, or $n = 2^k - 8$, or $n = 2^k$, the pure $[[n, n - \lceil \log_2 n \rceil - 2, 3]]$ code is optimal. If $2^{k-1} < n < \frac{2^{k+1}-1}{3}$, the pure $[[n, n - \lceil \log_2 n \rceil - 2, 3]]$ code is near optimal. If $n = 2^k - a$, where $a \in \{2, 4, 6, 10\}$, the pure $[[n, n - \lceil \log_2 n \rceil - 3, 3]]$ code is near optimal.

$$H_{14} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \varphi(1) & \varphi(2) & \varphi(3) & \varphi(4) & \varphi(8) & \varphi(12) & \varphi(18) & \varphi(22) & \varphi(26) & \varphi(30) & \varphi(32) & \varphi(33) & \varphi(34) & \varphi(35) \end{pmatrix},$$

$$G_1 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \varphi(6) & \varphi(7) & \varphi(14) & \varphi(15) & \varphi(16) & \varphi(17) & \varphi(24) & \varphi(25) \end{pmatrix},$$

$$G_2 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \varphi(20) & \varphi(21) & \varphi(28) & \varphi(29) & \varphi(38) & \varphi(39) & \varphi(46) & \varphi(47) \end{pmatrix},$$

$$G_3 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \varphi(40) & \varphi(41) & \varphi(42) & \varphi(43) & \varphi(48) & \varphi(49) & \varphi(50) & \varphi(51) \end{pmatrix},$$

$$G_4 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \varphi(52) & \varphi(53) & \varphi(54) & \varphi(55) & \varphi(60) & \varphi(61) & \varphi(62) & \varphi(63) \end{pmatrix}.$$

TABLE I
COMPARING QUANTUM CODES OF MINIMUM DISTANCE THREE. THE $[[n,k,3]]$CODES IN COLUMN 1 ARE OUR NEAR-OPTIMAL CODES, THE $[[n',k',3]]$ CODES IN COLUMN 2 ARE CODES OBTAINED IN [1], [5], [11], AND COLUMN 3 LISTS THE REFERENCE AND NOTATION

$[[34,26,3]]$	$[[35,26,3]]$	[5]
$[[62,53,3]]$	$[[63,54,3]]$	[1], [5]
$[[72,63,3]]$	$[[72,62,3]]$	[5]
$[[74,65,3]]$	$[[74,63,3]]$	[11]
$[[84,75,3]]$	$[[84,69,3]]$	[5]
$[[118,108,3]]$	$[[117,105,3]]$	[1]
$[[118,108,3]]$	$[[118,104,3]]$	[11]
$[[136,126,3]]$	$[[136,124,3]]$	[5]
$[[272+8i,261+8i,3]]$	$[[270+8i,257+8i,3]]$	[5] for $0 \le i \le 10$

2) For $12 \le n \le 32$, or $n = 8$, the pure codes with parameters $[[8,3,3]]$, $[[16,10,3]]$, $[[20,13,3]]$, $[[24,17,3]]$, and $[[32,25,3]]$ are optimal, whereas the pure codes with parameters $[[12,5,3]]$, $[[18,10,3]]$, $[[22,14,3]]$, $[[26,18,3]]$, $[[28,20,3]]$, and $[[30,22,3]]$ are near optimal.

Remark: Unlike previously known additive quantum codes (pure or impure) in [1]–[11], our pure optimal codes in the sense of Definition 1.1 are optimal. Though the $[[20,13,3]]$ code is near optimal in the sense of Proposition 1.1, from [2] we know that it is optimal. And the $[[18,10,3]]$ code does not achieve the near-optimal condition of Proposition 1.1, but from [2] we know that it is near optimal, because the optimal $[[18,11,3]]$ code is near optimal in the sense of Proposition 1.1. Thus, one can see that Proposition 1.1 is sufficient, but not necessary.

Theorem 10 of [2] is a special case of our Theorem 2.1. Our near-optimal $[[40,32,3]], [[168,158,3]] \cdots$ codes are not as good as the optimal $[[40,33,3]], [[168,159,3]] \cdots$ codes obtained by [2, Theorem 11], and our near-optimal $[[12,5,3]]$, $[[22,14,3]]$, $[[26,18,3]]$, $[[28,20,3]]$, $[[30,22,3]]$, $[[264,253,3]]$ codes are not as good as the corresponding optimal codes obtained in [2], [5]. However, many of our near-optimal quantum codes are better than or comparable with previously known codes in [1], [5], [11], see Table I. Thus, [2, Theorem 11] is partly generalized.

TABLE II
COMPARING QUANTUM CODES OF MINIMUM DISTANCE FOUR. THE $[[n,k,4]]$CODES IN COLUMN 1 ARE OUR CODES, THE $[[n',k',4]]$ CODES IN COLUMN 2 ARE CODES OBTAINED IN [1], [2], [5], AND COLUMN 3 LISTS THE REFERENCE AND NOTATION

$[[8,0,4]]$	$[[8,0,4]]$	[2]
$[[16,6,4]]$	$[[16,6,4]]$	[2]
$[[56,42,4]]$	$[[56,36,4]]$	[5]
$[[64,50,4]]$	$[[63,48,4]]$	[1]
$[[72,56,4]]$	$[[73,55,4]]$	[1]
$[[80,64,4]]$	$[[80,60,4]]$	[5]
$[[86,70,4]]$	$[[85,69,4]]$	[1], [2]
$[[88+8i,72+8i,4]]$	$[[88+8i,68+8i,4]]$	[5] for $0 \le i \le 5$
$[[136,118,4]]$	$[[136,116,4]]$	[5]

From [1]–[11], one can see the following. For n not too large, many of our quantum codes of minimal distance four are very good. However, when n increases, our quantum codes of minimal distance four become worse. Even so, some of our quantum codes of minimal distance four are better than or comparable with previously known codes in [1], [2], [5], [11]. For convenience, we use Table II to list them.

ACKNOWLEDGMENT

The authors are very grateful to the anonymous referees for their valuable comments and suggestions, which helped to improve the manuscript significantly.

$$H_{14}(m) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \varphi(1) & \varphi(2) & \varphi(3) & \varphi(4) & \varphi(8) & \varphi(12) & \varphi(18) & \varphi(22) & \varphi(26) & \varphi(30) & \varphi(32) & \varphi(33) & \varphi(34) & \varphi(35) \end{pmatrix} = \begin{pmatrix} H_{14} \\ \mathbf{0}_{(k-6)\times 14} \end{pmatrix}.$$

$$H_{12} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \varphi(0) & \varphi(1) & \varphi(2) & \varphi(3) & \varphi(6) & \varphi(7) & \varphi(12) & \varphi(13) & \varphi(16) & \varphi(17) & \varphi(24) & \varphi(25) \end{pmatrix}.$$

$$H_{12}(m) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \varphi(0) & \varphi(1) & \varphi(2) & \varphi(3) & \varphi(6) & \varphi(7) & \varphi(12) & \varphi(13) & \varphi(16) & \varphi(17) & \varphi(24) & \varphi(25) \end{pmatrix} = \begin{pmatrix} H_{12} \\ \mathbf{0}_{(k-5)\times 12} \end{pmatrix}.$$

References

[1] J. Bierbrauer and Y. Edel, “Quantum twisted codes,” *J. Combin. Des.*, vol. 8, pp. 174–188, 2000.

[2] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, “Quantum error-correction via codes over GF(4),” *IEEE. Trans. Inform. Theory*, vol. 44, pp. 1369–1387, July 1998.

[3] A. R. Calderbank and P. W. Shor, “Good quantum error-correcting codes exist,” *Phys. Rev. A*, vol. 54, pp. 1098–1105, Aug. 1996.

[4] H. Chen, “Some good quantum error-correcting codes from algebric geometric codes,” *IEEE. Trans. Inform. Theory*, vol. 47, pp. 2059–2061, July 2001.

[5] H. Chen, S. Ling, and C. P. Xing, “Quantum codes from concatenated algebric geometric codes,” preprint, 2001.

[6] D. Gottesman, “A class of quantum error-correcting codes saturating the quantum Hamming bound,” *Phys. Rev. A*, vol. 54, pp. 1862–1868, 1996.

[7] F. J. MacWillams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdan, The Netherlands: North-Holland, 1977.

[8] P. W. Shor, “Scheme for reducing decoherence in quantum computer memory,” *Phys. Rev. A*, vol. 52, pp. R2493–2496, Oct. 1995.

[9] A. M. Steane, “Error correcting codes in quantum theory,” *Phys. Rev.Lett.*, vol. 77, pp. 793–797, July 1996.

[10] ——, “Quantum Reed–Muller codes,” *IEEE. Trans. Inform. Theory*, vol. 45, pp. 1701–1703, July 1999.

[11] ——, “Enlargement of Calderbank–Shor–Steane quantum codes,” *IEEE. Trans. Inform. Theory*, vol. 45, pp. 2492–2495, Nov. 1999.

[12] V. Pless, “A classification of self-orthogonal codes over GF(2),” *Discr. Math.*, vol. 3, pp. 209–246, 1972.

Time Intervals and Counting in Point Processes

Bernard Picinbono, *Life Fellow, IEEE*

***Abstract*—Time point processes can be analyzed in two different ways: by the number of points in arbitrary time intervals or by distance between points. This corresponds to two distinct physical devices: counting or time-interval measurements. We present an explicit calculation, valid for arbitrary regular processes, of the statistical properties of time intervals such as residual or life time in terms of counting probabilities. For this calculation, we show that these intervals must be considered as random variables defined by conditional distributions.**

***Index Terms*—Counting, point processes, time measurements.**

I. Introduction

Point processes play an important role in many areas of physics and information sciences. They appear on a microscopic scale in the description of particle emission, and, for example, optical communication at a very low level of intensity requires the use of statistical properties of photons or photoelectrons [1], [2]. On the other hand, at a macroscopic level many areas such as traffic problems or computer communications require the use of point process statistics [3].

There are two approaches to describe point processes theoretically or to study them experimentally. The first one makes use of counting procedures in one or several nonoverlapping time intervals. The appropriate physical devices for this approach are counters. A limit aspect of counting appears in coincidence experiments in which the time intervals of counting are so small that they can only contain one or zero point [4].

On the other hand, it is possible to analyze point processes by using time intervals between points measurements. This introduces the concept of *residual time*, or survival time, or waiting time of order n, which is the time distance between an *arbitrary* time instant and the nth point of the processes following this instant. It is also possible to study the *life time* which is the time distance between successive or nonsuccessive points of the processes.

In the *stationary case*, the calculation of the probability distributions of residual or life times in terms of counting probabilities is known [5], [6]. However, in many practical situations, the stationarity assumption cannot be introduced and it appears that the direct transposition of the results obtained in the stationary case is not possible. The main reason is that time intervals must be considered as random variables (RV) defined by conditonal distributions. We shall see that this remark is of no importance in the stationary case but it must be taken into account for nonstationary processes. The omission of this fact has resulted in many incorrect expressions appearing in classical books on point processes. This is one of the reasons for analyzing the problem again and more carefully.

Before going further, let us introduce some general concepts and notation that will be used throughout the correspondence. As indicated in the title, we are interested in time point processes, which means that the points are *time instants*.

We assume that the point processes studied are defined only in a time interval (T_i, T), where T_i and T are the beginning and the end of the processes, respectively. For the sake of simplicity we take T_i as the origin of time, or $T_i = 0$.

We denote by $N[t_1, t_2)$ the number of points in the interval $[t_1, t_2)$. It is a discrete-valued RV and the point process is entirely defined if for any set of nonoverlapping intervals $[t_i, t_i + \Delta t_i)$ the joint probability distribution of the RVs $\{N[t_i, t_i + \Delta t_i)\}$ is known. These probabilities are denoted *counting probabilities*, and we shall use the notations

$$p_i(t, \tau) \triangleq P\{N[t, \tau) = i\}. \tag{1}$$

II. Residual Time of Order n

A. General Results

Let t be an arbitrary time instant satisfying $0 = T_i \leq t \leq T$. The residual time of order n is the RV $R_n(t)$ equal to the distance between the origin T_i and the nth point of the process posterior to t. It is *fundamental* to note that this RV does not exist if there are less than n points posterior to t, or if the event $N[t, T) < n$ is realized. Consequently, the distribution function (DF) of $R_n(t)$ defined by $F_n(t, \tau) = P[R_n(t) \leq \tau]$, $t \leq \tau \leq T$, is the conditional probability

$$\begin{aligned} F_n(t, \tau) &= P(\{N[t, \tau) \geq n\} | \{N[t, T) \geq n\}) \\ &= \frac{P(\{N[t, \tau) \geq n\} \cdot \{N[t, T) \geq n\})}{P(N[t, T) \geq n)}. \end{aligned} \tag{2}$$

As $\tau < T$, the numerator is equal to

$$P(N[t, \tau) \geq n) = 1 - \sum_{i=0}^{n-1} p_i(t, \tau). \tag{3}$$

The denominator has the same structure but $p_i(t, \tau)$ is replaced by $\pi_i = p_i(t, T)$. This yields

$$F_n(t, \tau) = \frac{1}{1 - \sum_{i=0}^{n-1} \pi_i} \left[1 - \sum_{i=0}^{n-1} p_i(t, \tau) \right]. \tag{4}$$

Manuscript received July 18, 2002; revised July 17, 2003. The material in this correspondence was presented in part at the GRETSI Conference (in French), Paris, France, September 2003.

The author is with the Laboratoire des Signaux et Systèmes (L2S), Supélec, Plateau de Moulon, 91912, Gif sur Yvette, France (e-mail: bernard.picinbono@lss.supelec.fr).

Communicated by A. Kavčić, Associate Editor for Detection and Estimation.
Digital Object Identifier 10.1109/TIT.2004.828081

0018-9448/04$20.00 © 2004 IEEE