and put $\hat{X}(t) = X(t) - x_0 I$. Then we have

$$\begin{aligned}\frac{\partial}{\partial t}\operatorname{Tr} f(X(t)) &= \sum_{n=0}^{\infty} a_n \operatorname{Tr}\frac{\partial}{\partial t}\hat{X}(t)^n \\ &= \sum_{n=1}^{\infty} a_n \sum_{i=1}^{n} \operatorname{Tr}\left(\hat{X}(t)\cdots\underbrace{\frac{\partial \hat{X}(t)}{\partial t}}_{i\text{th}}\cdots\hat{X}(t)\right) \\ &= \sum_{n=1}^{\infty} n a_n \operatorname{Tr}\left(\hat{X}(t)^{n-1}\frac{\partial}{\partial t}\hat{X}(t)\right) \\ &= \operatorname{Tr} f'(X(t))\frac{\partial X(t)}{\partial t}. \end{aligned}$$ □

Lemma 5: Let $A_i (i = 1, \cdots, a)$ be nonnegative linear operators on $\mathcal{H}$. If $0 < \alpha \leq \beta \leq 1$ then

$$\left(\sum_{i=1}^{a} \pi_i A_i^{1/\alpha}\right)^{\alpha} \geq \left(\sum_{i=1}^{a} \pi_i A_i^{1/\beta}\right)^{\beta}. \tag{22}$$

Proof: By Jensen's inequality for the operator concave function $x^{\gamma} (0 < \gamma \leq 1)$, it holds that

$$\sum_{i=1}^{a} \pi_i A_i \leq \left(\sum_{i=1}^{a} \pi_i A_i^{1/\gamma}\right)^{\gamma}.$$

Replace γ by α/β and A_i by $A_i^{1/\beta}$ in the above inequality, then

$$\sum_{i=1}^{a} \pi_i A_i^{1/\beta} \leq \left(\sum_{i=1}^{a} \pi_i A_i^{1/\alpha}\right)^{\alpha/\beta}.$$

Since x^{β} is a operator monotone function, we obtain

$$\left(\sum_{i=1}^{a} \pi_i A_i^{1/\beta}\right)^{\beta} \leq \left(\sum_{i=1}^{a} \pi_i A_i^{1/\alpha}\right)^{\alpha}.$$ □

ACKNOWLEDGMENT

The authors are grateful to the reviewers for their valuable comments and the editor for pointing out the existence of Winter's work. They also wish to thank Dr. K. Matsumoto for useful discussions, Prof. F. Hiai for his helpful comments about Lemmas 4 and 5 in the Appendix, and Prof. T.-S. Han for teaching them the history of the classical strong converse theorems.

REFERENCES

[1] A. S. Holevo, "The capacity of the quantum channel with general signal states," *IEEE Trans. Inform. Theory*, vol. 44, pp. 269–273, 1998 (originally appeared in LANL Rep., quant-ph/9611023, 1996.).
[2] B. Schumacher and M. D. Westmoreland, "Sending classical information via noisy quantum channels," *Phys. Rev. A*, vol. 56, pp. 131–138, 1997.
[3] P. Hausladen, R. Jozsa, B. Schumacher, M. D. Westmoreland, and W. K. Wootters, "Classical information capacity of a quantum channel," *Phys. Rev. A*, vol. 54, pp. 1869–1876, 1996.
[4] A. S. Holevo, "Bounds for the quantity of information transmitted by a quantum communication channel," *Probl. Inform. Transm.*, vol. 9, no. 3, pp. 177–183, 1973.
[5] H. P. Yuen and M. Ozawa, "Ultimate information carrying limit of quantum systems," *Phys. Rev. Lett.*, vol. 70, no. 4, pp. 363–366, 1993.
[6] A. S. Holevo, "Coding theorems for quantum channels," LANL Rep., quant-ph/9809023, 1998.
[7] A. Fujiwara and H. Nagaoka, "Operational capacity and pseudoclassicality of a quantum channel," *IEEE Trans. Inform. Theory*, vol. 44, pp. 1071–1086, 1998.
[8] G. Lindblad, "Completely positive maps and entropy inequalities," *Commun. Math. Phys.*, vol. 40, pp. 147–151, 1975.
[9] A. Uhlmann, "Relative entropy and the Wigner-Yanase-Dyson-Lieb concavity in an interpolation theory," *Commun. Math. Phys.*, vol. 54, pp. 21–32, 1977.
[10] A. S. Holevo, "On the capacity of quantum communication channel," *Probl. Inform. Transm.*, vol. 15, no. 4, pp. 247–253, 1979.
[11] J. Wolfowitz, "The coding of messages subject to chance errors," *Illinois J. Math.*, vol. 1, pp. 591–606, 1957.
[12] ——, "A note on the strong converse to the coding theorem for the general discrete finite memory channel," *Inform. Contr.*, vol. 3, pp. 89–93, 1963.
[13] S. Arimoto, "On the converse to the coding theorem for discrete memoryless channels," *IEEE Trans. Inform. Theory*, vol. IT-19, pp. 357–359, 1973.
[14] M. V. Burnashev and A. S. Holevo, "On reliability function of quantum communication channel," LANL Rep., quant-ph/9703013, 1997.
[15] R. G. Gallager, "A simple derivation of the coding theorem and some applications," *IEEE Trans. Inform. Theory*, vol. IT-11, pp. 3–18, 1965.
[16] R. Bhatia, *Matrix Analysis*. New York: Springer, 1997.
[17] F. Hansen and G. K. Pedersen, "Jensen's inequality for operators and Löwner's theorem," *Math. Ann.*, vol. 258, pp. 229–241, 1982.
[18] D. G. Luenberger, *Optimization by Vector Space Methods*. New York: Wiley, 1969.
[19] S. Verdú and T. S. Han, "A general formula for channel capacity," *IEEE Trans. Inform. Theory*, vol. 40, pp. 1147–1157,1994.
[20] A. Winter, "Coding theorem and strong converse for quantum channels," this issue, pp. 2481–2485.

Monotonicity of the Quantum Linear Programming Bound

Eric M. Rains

***Abstract*—The most powerful technique known at present for bounding the size of quantum codes of prescribed minimum distance is the quantum linear programming bound. Unlike the classical linear programming bound, it is not immediately obvious that if the quantum linear programming constraints are satisfiable for dimension K, then the constraints can be satisfied for all lower dimensions. We show that the quantum linear programming bound *is* monotonic in this sense, and give an explicitly monotonic reformulation.**

***Index Terms*—Quantum codes linear programming.**

I. INTRODUCTION

The most powerful technique known at present for bounding the size of quantum codes of prescribed minimum distance is the quantum linear programming (LP) bound:

Manuscript received March 29, 1998; revised January 18, 1999.
The author is with Shannon Laboratory, AT&T Research, Florham Park, NJ 07932-0971 USA (e-mail: rains@research.att.com).
Communicated by A. M. Barg, Associate Editor for Coding Theory.
Publisher Item Identifier S 0018-9448(99)08282-6.

0018–9448/99$10.00 © 1999 IEEE

Theorem (Quantum LP Bound): If there exists a quantum code $\mathcal{Q}$ encoding K states in n qubits, with minimum distance d, then there exist homogeneous polynomials $A(x,y)$, $B(x,y)$, and $S(x,y)$ of degree n, satisfying the equations

$$B(x,y) = A\left(\frac{x+3y}{2}, \frac{x-y}{2}\right) \tag{1}$$

$$S(x,y) = A\left(\frac{x+3y}{2}, \frac{y-x}{2}\right) \tag{2}$$

$$A(1,0) = K^2 \tag{3}$$

$$B(1,y) - \frac{1}{K}A(1,y) = O(y^d) \tag{4}$$

and the inequalities

$$A(x,y) \geq 0 \tag{5}$$

$$B(x,y) - \frac{1}{K}A(x,y) \geq 0 \tag{6}$$

$$S(x,y) \geq 0 \tag{7}$$

where $P(x,y) \geq 0$ means that the polynomial P has nonnegative coefficients.

Proof: This is [2, Theorem 10]; see also [4]. The polynomials $A(x,y)$, $B(x,y)$, and $S(x,y)$ are the weight enumerator, dual weight enumerator, and shadow enumerator, respectively, of the quantum code. □

Remark: In the sequel, we will use the standard notation $((n,K,d))$ to denote a quantum code encoding K states in n qubits, with minimum distance d.

It is clear that the existence of an $((n,K,d))$ code implies the existence of an $((n,K',d))$ code for all $K' \leq K$, which suggests that the same should be true for the quantum LP bound, namely, that if the quantum LP constraints can be satisfied for $((n,K,d))$, then they can be satisfied for $((n,K',d))$ for all $K' \leq K$. At first glance, this appears to be false; after all, in the inequality (6), decreasing K actually makes the inequality *harder* to satisfy. This impression is misleading, however; the quantum LP bound is indeed monotonic in K. To be precise

Theorem 1: Let n and d be integers, and let $1 \leq K' < K$ be real numbers. There exists a construction which, given a polynomial $A(x,y)$ satisfying the quantum LP constraints for $((n,K,d))$, produces a polynomial $\hat{A}(x,y)$ satisfying the quantum LP constraints for $((n,K',d))$.

II. Random Subcodes

The reason the quantum LP bound "ought" to be monotonic in K is that if $\mathcal{Q}$ is an $((n,K,d))$ code, and $\hat{\mathcal{Q}}$ is a subcode of $\mathcal{Q}$ of dimension K', then $\hat{\mathcal{Q}}$ is an $((n,K',d))$ code. Of course, in general, it is impossible to deduce the weight enumerators of $\hat{\mathcal{Q}}$ from the weight enumerators of $\mathcal{Q}$, so this is not directly applicable to the LP bound. However, if instead of picking a specific subcode, we average over *all* subcodes of a given dimension, the resulting average weight enumerators turn out to depend only on the original weight enumerators.

Recall that if $\mathcal{Q}$ is an $((n,K,d))$ code, and $P_{\mathcal{Q}}$ is the orthogonal projection onto $\mathcal{Q}$, then the weight enumerators $A_{\mathcal{Q}}(x,y)$ and $B_{\mathcal{Q}}(x,y)$ are defined by

$$A_{\mathcal{Q}}(x,y) = \sum_{e \in \mathcal{E}} \operatorname{Tr}(P_{\mathcal{Q}} e)^2 x^{n-\operatorname{wt}(e)} y^{\operatorname{wt}(e)}$$

$$B_{\mathcal{Q}}(x,y) = \sum_{e \in \mathcal{E}} \operatorname{Tr}(P_{\mathcal{Q}} e P_{\mathcal{Q}} e) x^{n-\operatorname{wt}(e)} y^{\operatorname{wt}(e)}$$

where $\mathcal{E}$ is the set of all tensor products of matrices from the set

$$\left\{ I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$$

and $\operatorname{wt}(e)$ is the number of nonidentity tensor factors in e.

Define

$$\hat{A}_{\mathcal{Q}}(x,y) = \boldsymbol{E}_{\hat{\mathcal{Q}} \subset \mathcal{Q}} A_{\hat{\mathcal{Q}}}(x,y)$$

and, similarly, for $\hat{B}_{\mathcal{Q}}(x,y)$, where $\boldsymbol{E}_{\hat{\mathcal{Q}} \subset \mathcal{Q}}$ denotes an average over subcodes $\hat{\mathcal{Q}}$ of dimension K'. (To be precise, the average is with respect to the unique probability distribution on subspaces of $\mathcal{Q}$ which is invariant under arbitrary unitary transformation.) Choose an orthonormal basis of $\mathcal{Q}$, and define a $2^n \times K$ matrix Π by taking the elements of the basis as columns. Then Π acts as a unitary isomorphism from $\mathbb{C}^K$ to $\mathcal{Q}$. So there exists a subspace $\mathcal{S}$ of $\mathbb{C}^K$ such that $\Pi(\mathcal{S}) = \hat{\mathcal{Q}}$; taking P' as the orthogonal projection onto that subspace, we have

$$P_{\mathcal{Q}} = \Pi \Pi^\dagger$$

$$P_{\hat{\mathcal{Q}}} = \Pi P' \Pi^\dagger$$

for some $K \times K$ projection operator P' of $\operatorname{rank} K'$; here $\dagger$ denotes the Hermitian transpose. So

$$\hat{A}_{\mathcal{Q}}(x,y) = \boldsymbol{E}_{P'} \sum_{e \in \mathcal{E}} \operatorname{Tr}(\Pi P' \Pi^\dagger e)^2 x^{n-\operatorname{wt}(e)} y^{\operatorname{wt}(e)}$$

and, similarly, for $\hat{B}_{\mathcal{Q}}$, where now the expectation is over $K \times K$ projection operators of $\operatorname{rank} K'$. Now, this clearly cannot depend on the basis we chose in defining Π. Thus for any $U \in U(K)$ (the group of $K \times K$ unitary operators), we have

$$\begin{aligned} \boldsymbol{E}_{P'} \operatorname{Tr}(\Pi P' \Pi^\dagger e)^2 &= \boldsymbol{E}_{P'} \operatorname{Tr}(\Pi U P' U^\dagger \Pi^\dagger e)^2 \\ &= \boldsymbol{E}_{P'} \boldsymbol{E}_{U \in U(K)} \operatorname{Tr}(\Pi U P' U^\dagger \Pi^\dagger e)^2 \end{aligned}$$

where $\boldsymbol{E}_{U \in U(K)}$ denotes expectation with respect to Haar distribution (the unique probability distribution on $U(K)$ invariant under multiplication by unitary matrices). In fact, since the unitary group acts transitively on subspaces of a fixed dimension, the expectation over P' is unnecessary, and we have

$$\begin{aligned} \boldsymbol{E}_{P'} \operatorname{Tr}(\Pi P' \Pi^\dagger e)^2 &= \boldsymbol{E}_{U \in U(K)} \operatorname{Tr}(\Pi U P' U^\dagger \Pi^\dagger e)^2 \\ &= \boldsymbol{E}_{U \in U(K)} \operatorname{Tr}(\Pi^\dagger e \Pi U P' U^\dagger)^2. \end{aligned}$$

At this point, we can apply the following lemma:

Lemma 2: Define functions

$$s_2(A) = \frac{1}{2}(\operatorname{Tr}(A)^2 + \operatorname{Tr}(A^2))$$

$$s_{1^2}(A) = \frac{1}{2}(\operatorname{Tr}(A)^2 - \operatorname{Tr}(A^2)).$$

For any $K \times K$ matrices A and B $(K > 1)$

$$\boldsymbol{E}_{U \in U(K)} s(AUBU^\dagger) = \frac{s(A)s(B)}{s(I_K)}$$

where s is either s_2 or s_{1^2}.

Proof: In fact, this is just the special case (in degree 2) of the more general fact

$$s_\lambda(I_K) \boldsymbol{E}_{U \in U(K)} s_\lambda(AUBU^\dagger) = s_\lambda(A) s_\lambda(B),$$

where λ is an arbitrary partition, and s_λ is the Schur function [1] of type λ. See, e.g., [1, Sec. VII.5, in particular example 3].

To be precise, that reference (and, indeed, most references on the subject) only states the result when A and B are positive semidefinite Hermitian, which is thus slightly weaker than we need. However, the equations are *polynomial* identities in the coefficients of A and B (in

our case of degree 2). So if we apply the result with $A = A_1 + tA_2$, with A_1 and A_2 positive semidefinite, we obtain an identity for all $t > 0$, and so for all t. Taking $t = -1$ then $t = \sqrt{-1}$, we find that the equation is valid in general. □

In particular

$$\begin{aligned}\boldsymbol{E}_{U\in U(K)} \operatorname{Tr}(\Pi^\dagger e \Pi U P' U^\dagger)^2 &= \boldsymbol{E}_{U\in U(K)} s_2(\Pi^\dagger e \Pi U P' U^\dagger) + s_{1^2}(\Pi^\dagger e \Pi U P' U^\dagger) \\ &= \frac{K'^2 + K'}{K^2 + K} s_2(\Pi^\dagger e \Pi) + \frac{K'^2 - K'}{K^2 - K} s_{1^2}(\Pi^\dagger e \Pi).\end{aligned}$$

In other words

Theorem 3: Let $\mathcal{Q}$ be a $((n, K, d))$ quantum code, with enumerators $A_\mathcal{Q}$ and $B_\mathcal{Q}$. Then the polynomials $\hat{A}_\mathcal{Q}$ and $\hat{B}_\mathcal{Q}$, defined as the average enumerators of subcodes of $\mathcal{Q}$ of dimension K', can be computed as

$$\begin{aligned}\hat{A}_\mathcal{Q}(x, y) &= \frac{K'(K'K - 1)}{K^3 - K} A_\mathcal{Q}(x, y) + \frac{K'(K - K')}{K^3 - K} B_\mathcal{Q}(x, y) \\ \hat{B}_\mathcal{Q}(x, y) &= \frac{K'(K - K')}{K^3 - K} A_\mathcal{Q}(x, y) + \frac{K'(K'K - 1)}{K^3 - K} B_\mathcal{Q}(x, y).\end{aligned}$$

This motivates the following guess for the polynomial $\hat{A}$ of Theorem 1:

Proof of Theorem 1: Define the new polynomial $\hat{A}$ by

$$\hat{A}(x, y) = \frac{K'(K'K - 1)}{K^3 - K} A(x, y) + \frac{K'(K - K')}{K^3 - K} B(x, y).$$

We need to show that $\hat{A}$ satisfies the quantum LP constraints for K'. Straightforward computation gives

$$\begin{aligned}\hat{A} &= \frac{K'^2}{K^2} A + \frac{K'(K - K')}{K^3 - K}\left(B - \frac{1}{K} A\right) \\ \hat{B} - \frac{1}{K'}\hat{A} &= \frac{K'^2 - 1}{K^2 - 1}\left(B - \frac{1}{K} A\right) \\ \hat{S} &= \frac{K'^2 + K'}{K^2 + K}\left(\frac{S(x, y) + S(-x, y)}{2}\right) \\ &\quad + \frac{K'^2 - K'}{K^2 - K}\left(\frac{S(x, y) - S(-x, y)}{2}\right).\end{aligned}$$

Since all of the constants appearing above are nonnegative for $1 \le K' < K$, and $\hat{A}(1, 0) = K'^2$, the claim follows. □

Remarks:

1) It is worth pointing out that the proof of Theorem 1 is logically independent of the computation of $\hat{A}_\mathcal{Q}$. That is, the only role of that computation was to motivate our guess of $\hat{A}$; once we had the guess, its origins were irrelevant.
2) Since the operation $A \mapsto \hat{A}$ preserves the additional constraint $A(1, y) = 1 + O(y^d)$, it follows that the quantum LP bound for *pure* codes is alo monotonic in K.

Theorem 3 has the following corollary:

Corollary 4: The average weight enumerator of a random $((n, K))$ quantum code is

$$A(x, y) = \frac{K(4^n K - 2^n)}{4^n - 1} x^n + \frac{K(K - 2^n)}{4^n - 1}(x + 3y)^n.$$

Proof: We have $A(x, y) = \hat{A}_\mathcal{H}$, where $\mathcal{H}$ is the trivial quantum code consisting of the entire Hilbert space, with weight enumerator $4^n x^n$. □

III. A Reformulation

Lemma 2 suggests that we should be able to obtain a simpler formulation of the quantum LP bound by considering the polynomials

$$\begin{aligned}C(x, y) &= \frac{A(x, y) + B(x, y)}{K^2 + K} \\ D(x, y) &= \frac{A(x, y) - B(x, y)}{K^2 - K}\end{aligned}$$

(where $D(x, y)$ is only well-defined for $K > 1$), associated to s_2 and s_{1^2}, respectively. In particular, we have the following result.

Lemma 5: For any $1 < K' < K$, $\hat{C} = C$ and $\hat{D} = D$.

So, if we reformulate the quantum LP bound in terms of C and D, the result should be explicitly monotonic, in that a feasible solution for K will itself be a feasible solution for all smaller K.

Theorem 6: If there exists an $((n, K, d))$ quantum code $(K > 1)$, then there exist homogeneous polynomials $C(x, y)$ and $D(x, y)$ of degree n, satisfying the equations

$$C(x, y) = C\left(\frac{x + 3y}{2}, \frac{x - y}{2}\right) \tag{8}$$

$$D(x, y) = -D\left(\frac{x + 3y}{2}, \frac{x - y}{2}\right) \tag{9}$$

$$C(1, 0) = 1 \tag{10}$$

$$C(1, y) - D(1, y) = O(y^d) \tag{11}$$

and satisfying the inequalities

$$C(x, y) - \frac{K - 1}{2K}(C(x, y) - D(x, y)) \ge 0 \tag{12}$$

$$C(x, y) - D(x, y) \ge 0 \tag{13}$$

$$C\left(\frac{x + 3y}{2}, \frac{y - x}{2}\right) \ge 0 \tag{14}$$

$$D\left(\frac{x + 3y}{2}, \frac{y - x}{2}\right) \ge 0. \tag{15}$$

Proof: We have

$$\begin{aligned}A(x, y) &= K^2 C(x, y) \\ &\quad - \frac{K^2 - K}{2}(C(x, y) - D(x, y)) \\ B(x, y) - \frac{1}{K} A(x, y) &= \frac{K^2 - 1}{2}(C(x, y) - D(x, y)) \\ S(x, y) &= \frac{K^2 + K}{2} C\left(\frac{x + 3y}{2}, \frac{y - x}{2}\right) \\ &\quad + \frac{K^2 - K}{2} D\left(\frac{x + 3y}{2}, \frac{y - x}{2}\right).\end{aligned}$$

Equations (8) and (9) are clearly equivalent to (1), while (10) and (11) are together equivalent to (3) and (4). Similarly, the inequalities (12) and (13) are equivalent to (5) and (6), respectively.

For (14) and (15), it suffices to note that (8) and (9) imply

$$\begin{aligned}C\left(\frac{x + 3y}{2}, \frac{y - x}{2}\right) &= C\left(\frac{-x + 3y}{2}, \frac{y + x}{2}\right) \\ D\left(\frac{x + 3y}{2}, \frac{y - x}{2}\right) &= -D\left(\frac{-x + 3y}{2}, \frac{y + x}{2}\right).\end{aligned}$$

It follows that the two terms in the expression for $S(x, y)$ have disjoint support. So (7) becomes (14) and (15). □

Theorem 1 is an obvious corollary; K appears only in (12), and decreasing K in that equation only makes the constraint easier to satisfy. For pure codes, the additional constraint $C(1, y) = 1 + O(y^d)$ holds, and again monotonicity is obvious.

It should also be noted that this theorem carries over readily to nonbinary codes (see [3, Secs. 4 and 5] for the constraints of the nonbinary quantum LP bound); in particular, the quantum LP bound is monotonic for larger alphabet codes as well.

REFERENCES

[1] I. G. Macdonald, *Symmetric Functions and Hall Polynomials*, 2nd ed. Oxford, U.K.: Oxford Univ. Press, 1995.

[2] E. M. Rains, "Quantum shadow enumerators," this issue, pp. 2361–2366.

[3] ——, "Quantum weight enumerators," *IEEE Trans. Inform. Theory*, vol. 44, pp. 1388–1394, July 1998.

[4] P. W. Shor and R. Laflamme, "Quantum analog of the MacWilliams identities in classical coding theory," *Phys. Rev. Lett.*, vol. 78, pp. 1600–1602, 1997.

Enlargement of Calderbank–Shor–Steane Quantum Codes

Andrew M. Steane

***Abstract*— It is shown that a classical error correcting code $C = [n, k, d]$ which contains its dual, $C^{\perp} \subseteq C$, and which can be enlarged to $C' = [n, k' > k + 1, d']$, can be converted into a quantum code of parameters $[[n, k+k'-n, \min(d, \lceil 3d'/2 \rceil)]]$. This is a generalization of a previous construction, it enables many new codes of good efficiency to be discovered. Examples based on classical Bose–Chaudhuri–Hocquenghem (BCH) codes are discussed.**

***Index Terms*—BCH code, CSS code, quantum error correction.**

I. INTRODUCTION

Quantum information theory is rapidly becoming a well-established discipline. It shares many of the concepts of classical information theory but involves new subtleties arising from the nature of quantum mechanics [2], [23]. Among the central concepts in common between classical and quantum information is that of error correction, and the error-correcting code. Quantum error-correcting codes have progressed from their initial discovery [19], [20] and the first general descriptions [5], [20], [21] to broader analyses of the physical principles [3], [6], [9], [13] and various code constructions [6], [9], [10], [14], [17], [18], [22], [24]. A thorough discussion of the principles of quantum coding theory is offered in [7], and many example codes are given, together with a tabulation of codes and bounds on the minimum distance for codeword length n up to $n = 30$ quantum bits.

For larger n there is less progress, and only a few general code constructions are known. The first important quantum code construction is that of [5], [20], [21]. The resulting codes are commonly referred to as Calderbank–Shor–Steane (CSS) codes. It can be shown that efficient CSS codes exist as $n \to \infty$, but on the other hand, these codes are not the most efficient possible. I will present here a method which permits most CSS codes to be enlarged, without an attendant reduction in the minimum distance of the code. The resulting codes are therefore more efficient than CSS codes. The examples I will give are found to be among the most efficient quantum codes known, and enabled some of the bounds in [7] to be tightened. The code construction is essentially the same as that described for Reed–Muller codes in [24], the new feature is to understand how the method works and thus prove that it remains successful for a much wider class of code. After this some relevant theory of Bose–Chaudhuri–Hocquenghem (BCH) codes [4], [12], [15] will be given and used to construct a table of example quantum codes built by the new method. The codes are *additive* and *pure* in the nomenclature of [7]. A pure additive code is *nondegenerate* in the nomenclature of [9].

Manuscript received April 24, 1998; revised February 23, 1999. This work was supported by the Royal Society and by St. Edmund Hall, Oxford.

The author is with the Department of Physics, University of Oxford, Clarendon Laboratory, Oxford OX1 3PU, U.K.

Communicated by A. R. Calderbank, Editor-in-Chief.

Publisher Item Identifier S 0018-9448(99)07304-6.

II. QUANTUM CODING

Following [7], the notation $[[n, k, d]]$ is used to refer to a quantum error-correcting code for n qubits having 2^k codewords and minimum distance d. Such a code enables the quantum information to be restored after any set of up to $\lfloor (d-1)/2 \rfloor$ qubits has undergone errors. In addition, when d is even, $d/2$ errors can be detected. We restrict attention to the "worst case" that any defecting qubit (i.e., any qubit undergoing an unknown interaction) might change state in a completely unknown way, so all the error processes X, Z, and $Y = XZ$ must be correctable [8], [9], [13], [21].

A quantum error-correcting code is an eigenspace of a commutative subgroup of the group E of tensor products of Pauli matrices. The commutativity condition can be expressed [6], [7], [9], [24]

$$H_x \cdot H_z^T + H_z \cdot H_x^T = \mathbf{0} \tag{1}$$

where H_x and H_z are $(n - k \times n)$ binary matrices which together form the *stabilizer* $\mathcal{H} = (H_x|H_z)$. All vectors $(u_x|u_z)$ in the code (where u_x and u_z are n-bit strings) satisfy $H_x \cdot u_z + H_z \cdot u_x = 0$. These are generated by the generator $\mathcal{G} = (G_x|G_z)$ which, therefore, must satisfy

$$H_x \cdot G_z^T + H_z \cdot G_x^T = \mathbf{0}. \tag{2}$$

In other words, $\mathcal{H}$ may be obtained from $\mathcal{G}$ by swapping the X and Z parts, and extracting the dual of the resulting $(n+k) \times 2n$ binary matrix. The rows of G_x and G_z have length n, and the number of rows is $n + k$.

The weight of a vector $(u_x|u_z)$ is the Hamming weight of the bitwise or of u_x with u_z. The minimum distance d of the code $\mathcal{C}$ is the largest weight such that there are no vectors of weight $< d$ in $\mathcal{C} \setminus \mathcal{C}^{\perp}$, where the dual is with respect to the inner product

$$((u_x|u_z), (v_x|v_z)) \equiv u_x \cdot v_z + u_z \cdot v_x.$$

A *pure* code has furthermore no vectors of weight $< d$ in $\mathcal{C}$, apart from the zero vector.

The CSS code construction [5], [21] is to take classical codes C_1 and C_2 with $C_1^{\perp} \subseteq C_2$, and form

$$\mathcal{G} = \left(\begin{array}{c|c} G_1 & 0 \\ 0 & G_2 \end{array}\right) \qquad \mathcal{H} = \left(\begin{array}{c|c} H_2 & 0 \\ 0 & H_1 \end{array}\right) \tag{3}$$

where G_i and H_i are the classical generator and check matrices. The dual condition $C_1^{\perp} \subseteq C_2$ ensures that $H_1 \cdot H_2^T = H_2 \cdot H_1^T = 0$ and, therefore, the commutativity condition (1) is satisfied. If $C_1 = [n, k_1, d_1]$ and $C_2 = [n, k_2, d_2]$ then the minimum distance of the quantum code is $\min(d_1, d_2)$ and the number of rows in $\mathcal{G}$ is $k_1 + k_2$, leading to quantum code parameters $[[n, k_1 + k_2 - n, \min(d_1, d_2)]]$.

0018–9448/99$10.00 © 1999 IEEE