Now, it follows directly from the definition of $\mathcal{B}_p(r,\, m)^{\perp}$ that if $f \in \langle E_p(r,\, m-1)\rangle$ then $f \cdot e_p(X_m) \in \mathcal{B}_p(r,\, m)^{\perp}$. Also, since

$$X_m^l = e_p(X_m) + (1 + e_p(X_m)) \cdot X_m^l$$

in $A_{p,\,m}$, $f_l \in \mathcal{B}_p(r-1,\, m-1)^{\perp}$ implies that $f_l \cdot X_m^l \in \mathcal{B}_p(r,\, m)^{\perp}$. Hence

$$B_p^1(r,\, m) \oplus B_p^2(r,\, m) \subseteq \mathcal{B}_p(r,\, m)^{\perp}.$$

Now

$$\dim(B_p^1(r,\, m)) = p \cdot \sum_{i=0}^{r-1} \binom{m-1}{i} (p-1)^i$$

and

$$\dim(B_p^2(r,\, m)) = \binom{m-1}{r} (p-1)^r.$$

The identity $\binom{m-1}{i} + \binom{m-1}{i-1} = \binom{m}{i}$ then implies that

$$\dim(B_p^1(r,\, m) \oplus B_p^2(r,\, m)) = \dim(\mathcal{B}_p(r,\, m)^{\perp}). \qquad \square$$

ACKNOWLEDGMENT

The authors wish to thank the referees and the Associate Editor for their helpful comments and suggestions.

REFERENCES

[1] E. F. Assmus Jr., "Bermans characterization of the Reed–Muller codes," *J. Statist. Planning Infer.*, vol. 56, pp. 17–21, 1996.
[2] Y. Berger and Y. Be'ery, "Bounds on the trellis size of linear block codes," *IEEE Trans. Inform. Theory*, vol. 39, pp. 203–209, Jan. 1993.
[3] ——, "Trellis-orientated decomposition and trellis complexity of composite-length cyclic codes," *IEEE Trans. Inform. Theory*, vol. 41, pp. 1185–1191, July 1995.
[4] S. D. Berman, "On the theory of group codes," *Kibernetika*, vol. 3, pp. 31–39, 1967.
[5] ——, "Semisimple cyclic and Abelian codes II," *Kibernetika*, vol. 3, pp. 21–30, 1967.
[6] T. Blackmore and G. H. Norton, "On the trellis structure of GRM codes," in *Proc. 6th Int. Workshop on Algebraic and Combinatorial Coding Theory*, 1998, pp. 26–29.
[7] ——, "On the state complexity of some long codes," in *Finite Fields: Theory, Applications and Algorithms*. Providence, RI: Amer. Math. Soc., 1999, vol. 225 of Contemporary Mathematics, pp. 203–214.
[8] ——, "On trellis structures for Reed–Muller codes," *J. Finite Fields Their Applic.*, vol. 6, pp. 39–70, 2000.
[9] I. F. Blake and R. C. Mullin, *The Mathematical Theory of Coding*. New York: Academic, 1975.
[10] J. C. Burkill and H. Burkill, *A Second Course in Mathematical Analysis*. Cambridge, U.K.: Cambridge Univ. Press, 1970.
[11] P. Camion, "Abelian Codes," Math. Res. Ctr., Univ. Wisconsin, Madison, Tech. Rep. 1059, 1971.
[12] P. Delsarte, "Automorphisms of Abelian codes," *Phillips Res. Repts.*, vol. 25, pp. 389–403, 1970.
[13] ——, "Weights of p-ary Abelian codes," *Phillips Res. Repts.*, vol. 26, pp. 145–156, 1971.
[14] B. M. Dwork and R. M. Heller, "Results of a geometric approach to the theory and construction of nonbinary multiple error and failure correcting codes," *IRE Nat. Conv. Rec*, pp. 123–129, 1959.
[15] G. D. Forney Jr., "Coset codes—Part II: Binary lattices and related codes," *IEEE Trans. Inform. Theory*, vol. 34, pp. 1152–1187, Sept. 1988.
[16] P. Heijnen and R. Pellikaan, "Generalized Hamming weights of q-ary Reed–Muller codes," *IEEE Trans. Inform. Theory*, vol. 44, pp. 181–196, Jan. 1998.
[17] J. M. Jensen, "On the concatenated nature of cyclic and Abelian codes," *IEEE Trans. Inform. Theory*, vol. IT-31, pp. 788–793, Nov. 1985.
[18] T. Kasami, T. Takata, T. Fujiwara, and S. Lin, "On complexity of trellis structure of linear block codes," *IEEE Trans. Inform. Theory*, vol. 39, pp. 1057–1064, May 1993.
[19] ——, "On the optimum bit orders with respect to state complexity of trellis diagrams for binary linear codes," *IEEE Trans. Inform. Theory*, vol. 39, pp. 242–245, Jan. 1993.
[20] F. J. MacWilliams, "Binary codes which are ideals in the group algebra of an Abelian group," *Bell Syst. Tech. J.*, vol. 44, pp. 987–1011, 1970.
[21] D. J. Muder, "Minimal trellises for block codes," *IEEE Trans. Inform. Theory*, vol. 34, pp. 1049–1053, Sept. 1988.
[22] A. Vardy, "Trellis structure of codes," in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands, 1998, ch. 24.
[23] J. K. Wolf, "Efficient maximum likelihood decoding of linear block codes using a trellis," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 76–80, Jan. 1978.

Concatenated Codes with Fixed Inner Code and Random Outer Code

Alexander Barg, Jørn Justesen, *Member, IEEE*, and Christian Thommesen, *Member, IEEE*

***Abstract*—We derive lower bounds on the distance and error exponent of the coding scheme described in the title. The bounds are compared to the parameters and error performance of a concatenated code family with varying inner codes of equal rates and a fixed minimum-distance separable (MDS) code as the outer code, letting the inner and outer code lengths approach infinity.**

***Index Terms*—Error exponent, minimum distance, power moment identities, weight distribution.**

I. INTRODUCTION: CONCATENATED CODES

The concatenated code construction is formed of an outer $[N, K]_{q^k}$ linear block code A and an inner $[n, k]_q$ code B by the following mapping:

$$\mathbb{F}_{q^k}^K \xrightarrow{A} \mathbb{F}_{q^k}^N \hookrightarrow \left(\mathbb{F}_q^k\right)^N \xrightarrow{B} \left(\mathbb{F}_q^n\right)^N \tag{1}$$

where the middle arrow denotes the standard embedding. The image of the composite mapping is called a concatenated code, and we denote it by $C = A \boxtimes B$. It is convenient to think of a code vector in C as an $n \times N$ matrix whose columns are vectors in B. Thus, C is an $[nN, kK]$ q-ary linear code. It is known that if both A and B are chosen randomly with uniform distribution from their respective ensembles and both n and N go to infinity, then almost all concatenated codes $C = A \boxtimes B$ asymptotically meet the Gilbert–Varshamov (GV) bound [2]. Moreover, the same is valid even if A is a fixed minimum-distance separable (MDS) (say Reed–Solomon) code [3], [9]. By making n grow slower than N and taking varying inner and MDS outer codes, it is

Manuscript received March 6, 2000. The material in this correspondence was presented in part at the IEEE International Symposium on Information Theory, Trondheim, Norway, 1994.

A. Barg is with Bell Laboratories, Lucent Technologies, Murray Hill, NJ 07974, USA (e-mail: abarg@research.bell-labs.com).

J. Justesen is with the Department of Telecommunication, Technical University of Denmark, DK 2800 Lyngby, Denmark (e-mail: jju@tele.dtk.dk).

C. Thommesen is with the Department of Mathematical Sciences, Aalborg University, DK 9220 Aalborg Ø, Denmark; (e-mail: cthom@math.auc.dk).

Communicated by R. Roth, Associate Editor for Coding Theory.

Publisher Item Identifier S 0018-9448(01)00372-8.

possible to present families of codes with both nonvanishing rate and distance and low construction complexity [11], [5]. Improvements of the parameters of these families are based on multilevel concatenations [3] and the use of algebraic geometry codes [6]. A detailed account of the early work is given in [3]; see also overviews in [4] and [1].

For a given rate $R \in [0,1]$ denote by $\delta_0 = \delta_0(R)$ the GV distance, i.e., the smaller root of the equation $R = \ln q - H_q(\delta)$, where

$$H_q(x) = x\ln(q-1) - x\ln x - (1-x)\ln(1-x)$$

is the entropy function. Suppose the constituent codes A and B are both chosen from their respective ensembles, and $r = (\ln q)k/n$ is the rate of the code B. This defines an ensemble of concatenated codes of rate $R = rK/N$. For this ensemble to contain codes meeting the GV bound it is sufficient that [3], [9]

$$r \geq \ln[q(1-\delta_0(R))]. \tag{2}$$

The same holds true if A is MDS. The error exponent of these codes for transmission over the q-ary symmetric channel with symbol-to-symbol error probability $p/(q-1)$ both in the case that A is a random code [3] and an MDS code [10] meets the random coding bound

$$E(R,p) \geq \begin{cases} -\delta_0 \ln \pi_q(p), & 0 \leq p \leq p_e \quad \text{(a)} \\ \ln q - R - \ln(1+(q-1)\pi_q(p)), & p_e \leq p \leq p_c \quad \text{(b)} \\ T_q(\delta_0, p) - \ln q + R, & p_c \leq p \leq \delta_0. \quad \text{(c)} \end{cases} \tag{3}$$

Here

$$\begin{aligned} p_e &= \frac{(2q - q\delta_0 - 2) - 2\sqrt{(q-1)(q-1-q\delta_0)}}{q^2(1-\delta_0)} \\ p_c &= \frac{\delta_0^2}{q\delta_0^2 + (q-1)(1-2\delta_0)} \\ \pi_q(p) &= p\frac{q-2}{q-1} + 2\sqrt{\frac{p(1-p)}{q-1}} \\ T_q(\mu, p) &= \mu\ln(q-1) - \mu\ln p - (1-\mu)\ln(1-p). \end{aligned} \tag{4}$$

An interesting question is what happens to the parameters of the family C if we relax (2) and take r to be a certain fixed value that does not depend on the target rate R. Then, clearly, R is at most r. As shown in [3] and [10], the attainable parameters then behave as

$$\delta_1(R) = \begin{cases} \delta_0(R), & r \geq \ln[q(1-\delta_0(R))] \\ \frac{R-r}{\ln(q/e^r - 1)}, & \text{otherwise} \end{cases} \tag{5}$$

where the second part of the bound is a segment of the straight line that is tangent to $\delta_0(R)$ at the point $R = \ln q - H_q(1 - e^r/q)$ and connects it to the point $(r, 0)$.

In this correspondence, we further relax the conditions and address the following problem: what are the parameters of C if B is a fixed linear $[n,k]_q$ code and the code A is chosen randomly from the ensemble of $[N,K]_{q^k}$ linear codes. In the next section, we derive a lower existence bound on the asymptotic parameters of C and compare it to the GV bound and to the bound (5). In Section III, we derive an upper bound on the weight spectrum of C and estimate its error probability of decoding under the maximum-likelihood (ML) algorithm. The exponent of this probability is compared to the random coding exponent.

II. Parameters of the Coding Scheme

Suppose that in (1) we take A to be a random linear q^k-ary code and B a certain fixed $[n,k]_q$ linear code with weight distribution $\boldsymbol{A} = [A_0, A_1, \ldots, A_n]$. More specifically, if G_O is the generator matrix of A, we assume each element in it is chosen independently with uniform distribution from $\mathbb{F}_{q^k}$. This defines an ensemble of concatenated codes $C = A \boxtimes B$; our goal will be to prove an existence bound on their parameters.

Let us introduce a random variable X defined by

$$P(X = i) = \frac{1}{q^k} A_i, \qquad i = 0, 1, \ldots, n. \tag{6}$$

In particular, if B is an $[n,n,1]_q$ all-word code, then the corresponding random variable X is binomially distributed; we denote it by X_0.

For a given nonzero information sequence $\boldsymbol{u} \in \mathbb{F}_{q^k}^K$, the weight W of the corresponding codeword is a random variable. It is conveniently expressed via X as follows.

Lemma 1: Let $\boldsymbol{u} \in \mathbb{F}_{q^k}^K \setminus \{\boldsymbol{0}\}$ be an information sequence. The Hamming weight W of the corresponding codeword in C equals

$$W = X_1 + X_2 + \cdots + X_N \tag{7}$$

where $X_i \sim X$, $i = 1, \ldots, N$ are independent and identically distributed (i.i.d.) random variables with distribution (6).

Let $R = (\ln q)kK/nN$. Strictly speaking, R is not the rate of C since G_O can have rank less that K, but as usual, for growing parameters almost all codes C have rate approaching R. In the next theorem we use (7) to derive an existence bound on the codes C from the defined ensemble.

Proposition 1: There exist concatenated codes C whose rate and relative distance approach (R, δ) if

$$nR < -\ln(E\{e^{-t(X-n\delta)}\}), \qquad t \geq 0.$$

Proof: The probability for a code in the ensemble to have a fractional Hamming weight at most δ is, for any $t \geq 0$, bounded above as follows:

$$\begin{aligned} & e^{RnN} P(X_1 + X_2 + \cdots + X_N \leq nN\delta) \\ & \quad \leq e^{RnN} E\{e^{-t(\sum X_i - nN\delta)}\} \\ & \quad = (e^{nR} E\{e^{-t(X-n\delta)}\})^N. \end{aligned}$$

□

Remark: The bound of this proposition does not depend on N. However, for $\delta \leq (q-1)/q$, Chernoff's theorem for large deviations gives

$$\lim_{N\to\infty} \frac{\ln(P(X_1 + \cdots + X_N \leq nN\delta))}{N} = \min_{t \geq 0} \ln(E\{e^{-t(X-n\delta)}\}). \tag{8}$$

So, by using the random technique together with the union bound for the minimum weight, no better result than Proposition 1 can be obtained asymptotically, if the inner code is fixed, and $N \to \infty$.

Let $\tau = \tau(\delta)$ be chosen so that

$$E\left\{e^{-\tau(X-n\delta)}\right\} = \min_{t \geq 0} E\left\{e^{-t(X-n\delta)}\right\}. \tag{9}$$

Computing $(\partial/\partial t) E\{e^{-t(X-n\delta)}\}$, we see that τ satisfies the following equation:

$$E\left\{(X - n\delta)e^{-\tau(X-\delta n)}\right\} = 0. \tag{10}$$

If τ is used as parameter for the (R, δ) curve, given by

$$R = -\frac{1}{n}\ln\left(E\left\{e^{-\tau(X-\delta n)}\right\}\right)$$

then (10) relates τ and δ. This gives rise to the following theorem.

Theorem 1: The random ensemble of codes C contains codes whose parameters approach the following bound:

$$R = \frac{1}{n}(\tau\phi'_\tau - \phi) \tag{12}$$

$$\delta = -\frac{1}{n}\phi'_\tau, \qquad \tau \geq 0 \tag{13}$$

where $\phi = \phi(X, \tau) := \ln E e^{-\tau X}$.

Proof: Solving (10) for δ, we obtain

$$\delta = \frac{1}{n}\frac{E\{Xe^{-\tau X}\}}{E\{e^{-\tau X}\}}.$$

Further, (11) gives

$$R = -\frac{1}{n}\ln Ee^{-\tau X} - \tau\delta.$$

Substituting δ completes the proof. □

Let us relate this bound to bounds $\delta_0(R)$ and $\delta_1(R)$ discussed above. The slope of δ plotted versus R equals $\delta'_\tau/R'_\tau = -1/\tau$. To gain understanding of the properties of the bound (12)–(13), let us compute its behavior as $R \to 0$ and $R \to r$. For $\tau = 0$, $(R, \delta) = (0, (q-1)/q)$ is obtained, so all the bounds δ_0, δ_1, and (12)–(13) coincide. Computing the limit for $\tau \to \infty$, we obtain $(R, \delta) \to (\frac{k}{n}\ln q, 0)$, which reflects the fact that minimum distance greater than zero can only be obtained when $R \le r$. Finally, it can be seen that the function $\delta(R)$ is strictly $\cup$-convex for $0 \le R \le r$. Indeed, we have

$$\delta''_{R^2} = \frac{\delta''_{\tau 2}R'_\tau - \delta'_\tau R''_{\tau 2}}{(R'_\tau)^3} = \frac{(\phi''_{\tau 2})^2}{n^2(R'_\tau)^3}.$$

It is straightforward to see that R is a growing function of the parameter τ, and so $\delta''_{R^2} > 0$.

Let $C_0 = A \boxtimes (\mathbb{F}_q)^n$ be a code with A random and B the $[n, n, 1]_q$ all-word code. Effectively, we eliminate the concatenated construction, and look at random q-ary codes. Then, Theorem 1 gives the GV bound. We isolate this in a separate lemma, whose proof is straightforward.

Lemma 2: Bound (12)–(13) with $X = X_0$ gives the GV bound.

Next let us compare (12)–(13) to $\delta_0(R)$ and $\delta_1(R)$ for an arbitrary inner code B.

Proposition 2: For a given rate $R \in (0, r]$, the distance (13) of the concatenated code C is always less than $\delta_0(R)$ and less than $\delta_1(R)$.

Proof: We use the Pless power moment identities for the coefficients of the weight distribution of a linear code [7]

$$\sum_{j=0}^{n}(n-j)^r A_j = \sum_{j=0}^{n} A_j^\perp \left(\sum_{\nu=0}^{r}\nu! S(r,\nu) q^{k-\nu}\binom{n-j}{n-\nu}\right), \qquad j \ge 0$$

where $S(r, \nu)$ are the Stirling numbers of the second kind ($S(r, \nu)$ is the number of partitions of an r-set into ν nonempty parts, and hence nonnegative). So, obviously, for any code B

$$E\{(n-X)^j\} \ge E\{(n-X_0)^j\}$$

with the equality for all $i = 0, 1, \ldots, d^\perp(B) - 1$. Writing out the power series in the neighborhood of $t = 0$, we observe that for any code different from the whole space $\mathbb{F}_q^n$

$$E\{e^{-t(X-n)}\} > E\{e^{-t(X_0-n)}\}$$

or that

$$E\{e^{-tX}\} > E\{e^{-tX_0}\}, \qquad t \ge 0. \tag{14}$$

From this we observe that $\phi(t, X) \ge \phi(t, X_0)$ for all $t \ge 0$. Now suppose that

$$\tau(B) = \arg\min_{t\ge 0} E(e^{-t(X-n\delta)})$$

is the value of τ for the code B and τ_0 is the same for the inner code $\mathbb{F}_q^n$. Since the rate of the code C is fixed, i.e., by (12)

$$\tau(B)\phi'_\tau(X, \tau(B)) - \phi(X, \tau(B)) = \tau_0\phi'_\tau(X_0, \tau_0) - \phi(X_0, \tau_0)$$

we finally obtain $\phi'_\tau(X, \tau(B)) > \phi'_\tau(X_0, \tau_0)$. This is the first part of our claim. The second part follows since both bounds (12)–(13) and δ_1 meet the R-axis at $R = r$ and since the former is convex and the latter a straight line.

Another proof of this proposition, similar to the above, but based on the MacWilliams identities, is given in Appendix A.

Bound (12)–(13) displays interesting behavior for small values of R. Let $u = (q-1/q) - \delta$ and let us write the expansion of the GV function $R = \ln q - H_q(\delta)$ in the neighborhood of $u = 0$. The derivatives of $H_q(\theta - x)$ are $H' = \ln(\theta - x)/((q-1)(1-\theta+x))$

$$\frac{d^s}{dx^s}H_q(\theta - x) = \frac{(-1)^{s-1}(s-2)!}{(1-\theta+x)^{s-1}} - \frac{(s-2)!}{(\theta-x)^{s-1}}, \qquad s \ge 2$$

where $\theta = (q-1)/q$. So we obtain, in the neighborhood of $u = 0$

$$R(\theta - u) = \sum_{s\ge 2}\left[\frac{q^{s-1}}{s(s-1)(q-1)^{s-1}} - \frac{(-q)^{s-1}}{s(s-1)}\right]u^s. \tag{15}$$

For $q = 2$ this takes a somewhat more appealing form

$$R((1/2) - u) = \sum_{\sigma\ge 1}(2u)^{2\sigma}/2\sigma(2\sigma - 1).$$

Now we are in a position to formulate our claim.

Proposition 3: Let B be a code with dual distance $d^\perp$. Then, first $d^\perp - 1$ terms in the power expansion of the bound (12)–(13) for $R \to 0$ coincide with the corresponding terms of (15).

The proof of this proposition is a straightforward though tedious calculation based on the fact that the rth-power moment of the weight distribution is equal to that of the "binomial" distribution as long as $A_r^\perp = 0$.

Though the expression for our bound is cumbersome, the bound itself is easily calculated. For instance, taking the $[24, 12]$ extended Golay code $\mathcal{G}_{24}$ with the weight distribution ($A_0 = A_{24} = 1, A_8 = A_{16} = 759, A_{12} = 2576$) as the inner code B, we obtain the bound plotted in Fig. 1 together with the GV bound and $\delta_1(R)$. In Fig. 2, the three bounds are compared for the $[12, 6]$ ternary Golay code $\mathcal{G}_{12}$ as code B.

III. Error Performance

Let us analyze the error performance of our coding scheme used for transmission over the q-ary symmetric channel with symbol-to-symbol error probability $p/(q-1)$ and decoded by the ML rule. We use the union bound together with estimates for the weight spectrum of C.

Generally, let $\mathcal{C}$ be a sequence of linear codes with weight spectrum A_w, $w \ge 0$. Suppose that the distance of $\mathcal{C}$ equals $d = \mu n$. Further, suppose that beginning with a certain value of the code length n the exponent of the number of codewords of a given weight $w = \omega n$ can be bounded above as

$$(1/n)\ln A_w \le \alpha(\omega).$$

Assuming that the the error probability of decoding for family $\mathcal{C}$ behaves exponentially in n and putting $P_{\mathrm{de}}(\mathcal{C}, p) \le \exp(-nE(R, p))$, one can bound $E(R, p)$ below as follows.

Proposition 4:

$$E(R, p) \ge -\max_{\mu\le\omega\le 1}(\alpha(\omega) + \omega\ln\pi_q(p)) \tag{16}$$

where $\pi_q(p)$ is defined in (4).

A sketch of the proof is given in Appendix B.

For instance, taking $\mathcal{C} = C_0$ to be a sequence of concatenated codes with a random outer code A and inner code $B = (\mathbb{F}_q)^n$, we obtain $\alpha(\omega) = H_q(\omega) + R - \ln q$ for $\omega \ge \delta_0(R)$. Substituting this in (16) produces parts (a) and (b) of (3) of the random coding exponent.

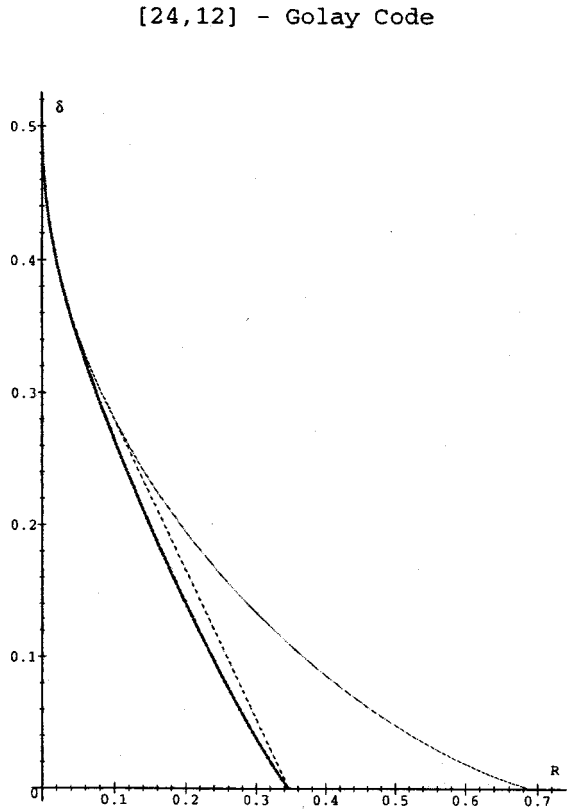

Fig. 1. The bold solid curve is the bound (12)–(13). The thin solid curve is the GV bound $(\delta_0(R))$. The dotted curve is $\delta_1(R)$. The tangent point of δ_1 and δ_0 is $R = 0.0884; \delta_0(0.0884) = \delta_1(0.0884) = 0.293$, and our bound gives $\delta(0.0884) = 0.281$.

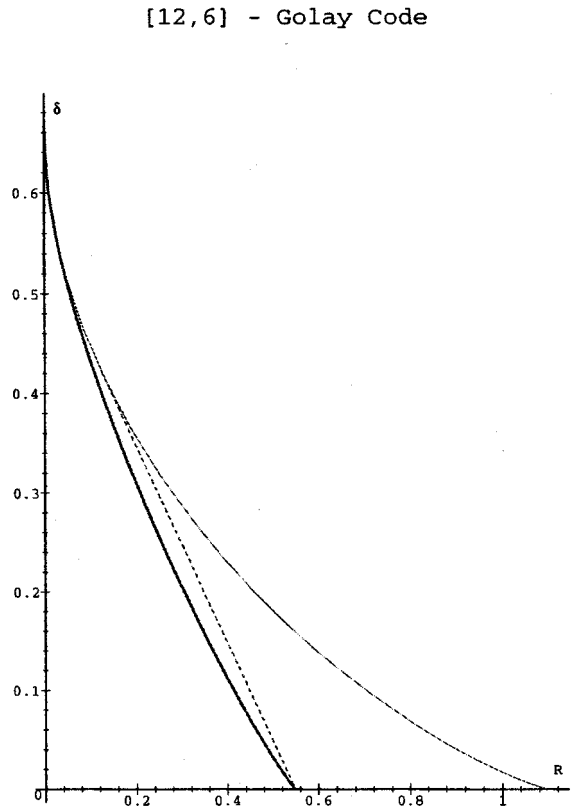

Fig. 2. The bold solid curve is the bound (12)–(13). The thin solid curve is the GV bound $(\delta_0(R))$. The dotted curve is $\delta_1(R)$. The tangent point of δ_1 and δ_0 is $R = 0.125; \delta_0(0.125) = \delta_1(0.125) = 0.423$, and our bound gives $\delta(0.125) = 0.401$.

It is known that for any code family that meets the GV bound for $R \to 0$, the error exponent in this neighborhood will behave as (a) in (3). It is also clear that for our family C with fixed inner code B the exponent $E(R, p)$ (at least, calculated by the union bound) will become zero for $R \geq r$. To estimate the error performance for $0 < R < r$ let us estimate the average weight distribution of a concatenated code C with inner code B with known weight distribution $(A_0, A_1, \ldots, A_n)$. The answer is given in the following theorem, which is proved exactly as Theorem 1.

Theorem 2: Let $E_N(\omega)$ be the average number of vectors of weight $\leq nN\omega$ over the ensemble of concatenated codes C. Then for $1 \geq \omega \geq \delta$,

$$\ln(E_N(\omega)/nN) \leq R + \frac{1}{n}(\ln \phi - \tau\phi'_\tau) \tag{17}$$

$$\omega = -\frac{1}{n}\phi'_\tau \tag{18}$$

where X is the random variable with

$$P(X = w) = A_w/q^k$$
$$\phi(X, \tau) = \ln E e^{-\tau X}$$

and τ is chosen from the condition

$$E\left(e^{-\tau(X-n\omega)}\right) = \min_{t \geq 0} E\left(e^{-t(X-n\omega)}\right).$$

This bound again is easy to compute. For instance, as a follow-up of the above example, let us compute the average exponent of the weight spectrum of the family of concatenated codes with $B = \mathcal{G}_{24}$. This is compared to the weight spectrum of $C_0 = A \boxtimes (\mathbb{F}_2)^n$ in Fig. 3, where on the horizontal axis we show the relative weight ω and on the vertical axis the logarithm of the weight distribution of the code

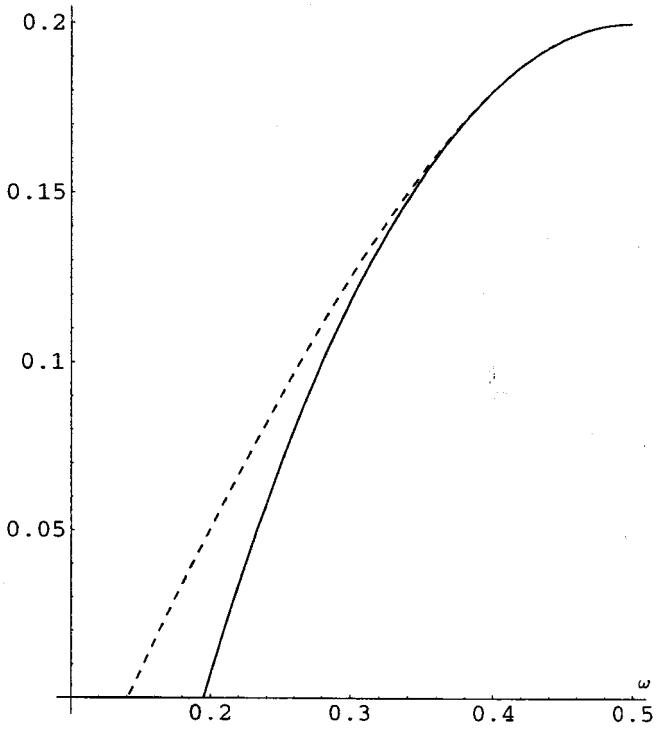

Fig. 3. The solid curve is the exponent of the weight spectrum of $C_0 = A \boxtimes (\mathbb{F}_q)^n$; the dashed curve is an upper bound on the exponent of the weight spectrum of $C = A \boxtimes \mathcal{G}_{24}$.

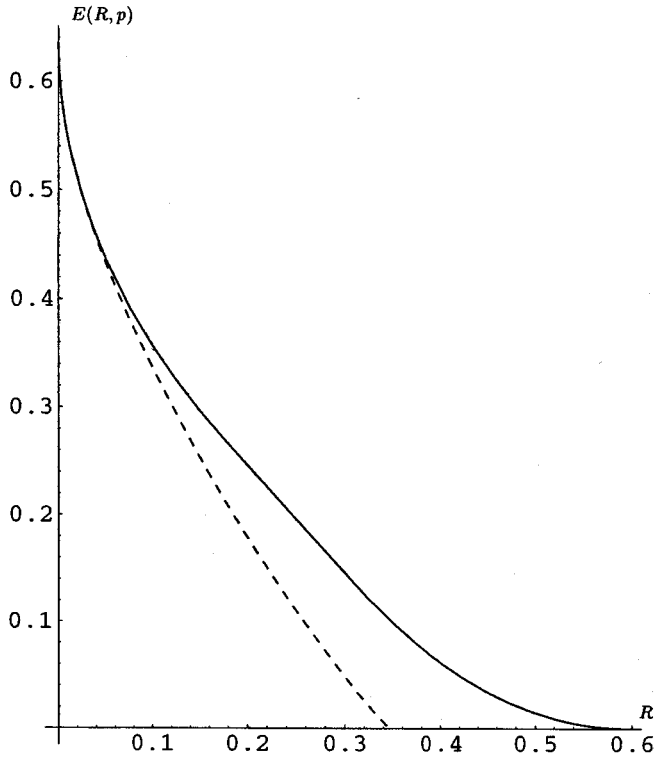

Fig. 4. The solid curve is the random coding exponent (3); the dashed curve is a lower bound on the error exponent of the family $C = A \boxtimes \mathcal{G}_{24}$. The channel error probability is $p = 0.02$.

divided by nN. Substituting the resulting weight distribution into (16), it is possible (and easy) to bound below the average error exponent of the family C. This bound is shown in Fig. 4 together with the random coding exponent (3).

Appendix A
Another Proof of Proposition 2

Let $(A_0^\perp, A_1^\perp, \ldots, A_n^\perp)$ be the MacWilliams transform of the weight distribution of B. The MacWilliams equation for the weight polynomials has the form

$$\frac{1}{q^k} A(z) = \sum_{j=0}^{n} A_j^\perp (q^{-1} + \theta z)^{n-j} (q^{-1} - z q^{-1})^j. \qquad (19)$$

Substituting $z = e^{-t}$ in (19), we obtain

$$E\{e^{-tX}\} = \sum_{j=0}^{n} A_j^\perp (q^{-1} + \theta e^{-t})^{n-j} (q^{-1} - e^{-t} q^{-1})^j.$$

In particular, taking $B = \mathbb{F}_q^n$, we obtain

$$E\{e^{-tX_0}\} = A_0^\perp (q^{-1} + \theta e^{-t})^n.$$

Combining the last two equations, we get

$$E\{e^{-tX}\} = E\{e^{-tX_0}\} + \sum_{j=d^\perp}^{n} A_j^\perp (q^{-1} + \theta e^{-t})^{n-j} (q^{-1} - e^{-t} q^{-1})^j.$$

Further, the sum on j on the right-hand side of this equality is nonnegative since for $t \geq 0$, $0 \leq q^{-1} - e^{-t} q^{-1} \leq t/q$. This takes us again to (14).

Appendix B
Proof of Proposition 4 (An Outline)

The proof proceeds by an application of the union bound. We compute the two-word error probability and multiply it by the number of codewords of weight w. This gives the following expression:

$$P_{\mathrm{de}}(\mathcal{C}, p) \leq \sum_{w=d}^{n} A_w \sum_{j=0}^{w} \sum_{i=\lceil \frac{w-j}{2} \rceil}^{w-j} \sum_{\ell=0}^{n-w} \binom{w}{i} \binom{w-i}{j} (q-2)^j \times \binom{n-w}{\ell} (q-1)^\ell \left(\frac{p}{q-1}\right)^{i+j+\ell} (1-p)^{n-i-j-\ell}.$$

Direct optimization shows that the exponent of the maximal term in the sum on j behaves as $n\omega \ln \pi_q(p)$. Now taking logarithms establishes (16).

As a side remark, note that in many cases the bound (16) can be improved for high code rates. The reason for this is that the union bound becomes too crude even compared to the trivial assumption that for all errors of weight greater than some r every error vector results in a decoding error. In particular, for $B = (\mathbb{F}_q)^n$ this argument produces the sphere-packing bound (c) of (3); see [8] for details.

References

[1] A. Barg, "Complexity issues in coding theory," in *Handbook of Coding Theory*, V. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier Science, 1998, vol. 1, pp. 649–754.

[2] E. L. Blokh and V. V. Zyablov, "Existence of linear concatenated binary codes with optimal correcting properties," *Probl. Pered. Inform.*, vol. 9, pp. 3–10, 1973.

[3] ——, *Linear Concatenated Codes*. Moscow, U.S.S.R.: Nauka, 1982. In Russian.

[4] I. Dumer, "Concatenated codes and their multilevel generalizations," in *Handbook of Coding Theory*, V. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier Science, 1998, vol. 2, pp. 1911–1988.

[5] J. Justesen, "A class of constructive asymptotically good algebraic codes," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 652–656, Sept. 1972.

[6] G. L. Katsman, M. A. Tsfasman, and S. G. Vlăduţ, "Modular curves and codes with a polynomial construction," *IEEE Trans. Inform. Theory*, vol. IT-30, pp. 353–355, Mar. 1984.

[7] V. Pless, *Introduction to the Theory of Error-Correcting Codes*. New York: Wiley, 1988.

[8] G. Sh. Poltyrev, "Bounds on the decoding error probability of binary linear codes via their spectra," *IEEE Trans. Inform. Theory*, vol. 40, pp. 1284–1292, July 1994.

[9] C. Thommesen, "The existence of binary linear concatenated codes with Reed-Solomon outer codes which asymptotically meet the Gilbert-Varshamov bound," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 850–853, Nov. 1983.

[10] ——, "Error-correcting capabilities of concatenated codes with MDS outer codes on memoryless channels with maximum-likelihood decoding," *IEEE Trans. Inform. Theory*, vol. IT-33, pp. 632–640, Sept. 1987.

[11] V. V. Zyablov, "An estimate of complexity of constructing binary linear cascade codes," *Probl. Pered. Inform.*, vol. 7, no. 1, pp. 3–10, 1971.