I. Introduction

J. von Neumann [1] raised the question of how systems with unreliable components can be used efficiently in a reliable way. The most important example known is which this program was carried out successfully, is Shannon's information theory. In another direction, Elias and Winograd studied the question whether reliable computation is possible at a positive rate in the presence of noise [3], [4].

Table I presents the parameters \( n, k, d \) for the five new codes \( C_d \), and for the \( A_{1d} \), \( 1 \leq i \leq 5, 1 \leq j \leq 6 \), required by Construction XX. Of the twenty codes \( A_{1d}, 1 \leq j \leq 4 \), all but \( A_{1d} \) and \( A_{1d} \) are cyclic. \( A_{1d} \) is a 5-dimensional subcode of \( A_{2d} \) that contains the vector of weight 31. Likewise, \( A_{1d} \sim A_{2d} + A_{3d} \) is a 10-dimensional subcode of \( A_{1d} \) containing the vector of weight 31. Of the remaining eighteen \( A_{1d}, 1 \leq j \leq 4 \), only ten are distinct.

Table II shows the roots of the check polynomial for these ten cyclic codes. For example, \( A_{2d} \) and \( A_{3d} \) are the same cyclic [31,6,15] code with check polynomial of degree 6 and having roots 1 and \( a \), where \( a \) is a primitive root of GF(32). \( A_{2d} \) is also a [31,6,15] cyclic code whose check polynomial has roots 1 and \( a \). \( A_{1d} \sim A_{2d} + A_{3d} \) is a [31,11,11] cyclic code whose check polynomial has roots 1, \( a \) and \( a^2 \). The check polynomials in Table II were selected to complement the generating polynomials listed in [3, App. D]. The ten codes \( A_{1d}, 5 \leq j \leq 6 \), are, for the most part, trivial. The existence of the [12,7,4] and [18,9,6] codes is guaranteed by the tables in [1] and [4].

Clearly Construction XX has further applications. The five codes, described here were selected to have \( d = 29 \), in order to enable comparison with the information in the table of [1].

II. Elias' Model

Two strings of data

\[ X_1 = (x_{11}, \cdots, x_{ik}), \quad X_2 = (x_{21}, \cdots, x_{2k}) \]

are to be encoded by two separate encoders \( E_1, E_2 \) into strings of length \( n \)

\[ E_1(X_1) = Y_1 = (y_{11}, \cdots, y_{1n}), \quad E_2(X_2) = Y_2 = (y_{21}, \cdots, y_{2n}). \]

The quantity of interest is

\[ f(X_1, X_2) = (f_1(x_{11}, x_{21}), f_2(x_{12}, x_{22}), \cdots). \]

However, the computation is done by a computer, operating on a bit-by-bit basis on \( Y_1, Y_2 \). In the presence of noise its computation would be

\[ F(Y_1, Y_2) = (f(Y_{11}, Y_{21}), \cdots) \triangleq Z = (z_1, \cdots, z_n). \]

In the presence of noise it produces instead

\[ Z^* = (z_1^*, \cdots, z_n^*) \triangleq Z + \text{noise}. \]

Here the noise is that of a binary symmetric channel. The decoder accepts \( Z^* \) as its input and performs the function \( D \) to obtain

\[ U \triangleq D(Z^*) = (u_1, \cdots, u_k). \]

The whole system performs reliably if \( U = f(X_1, X_2) \). Note that \( F \) can be different from \( f \).

Elias makes the following assumptions.
1) \( X_1 \) and \( X_2 \) are encoded independently.
2) In the absence of noise \( D \) is bijective.
3) \( F \) operates bit by bit.

These assumptions mean that \( Y_1 \) only carries information about \( X_1 \) \( (i = 1, 2) \) and does not carry information about logical combinations of the two blocks. Thus, none of the desired computation \( f(X_1, X_2) \) is done in the encoder, which is also assumed to be noiseless here, or in the decoder. This is to say that all calculations will be done by the computer.

1Thanks are due to A. El Gamal for drawing our attention to the work of these authors.
2A referee kindly points out that [11] and [12] give related results and extensions in a different direction, respectively.

This result was conjectured in [4, Abstract].
III. WINOGRAD'S RESULT AND PROOF

**Theorem:** Suppose that
\[ f(X_1, X_2) = f_1(x_{11}, x_{21}), \ldots, f_k(x_{1k}, x_{2k}) \]
and
\[ F(Y_1, Y_2) = (F_1(y_{11}, y_{21}), \ldots, F_k(y_{1k}, y_{2k})) \]

Then, in order to correct \( \epsilon n \) \( (0 < \epsilon < 1) \) errors, necessarily \( R = \frac{k}{n} \to 0 \) \( (n \to \infty) \).

**Lemma:** Let \( D^{-1}(X_1 \land X_2) = E_1(X_1) \land E_2(X_2) \) and let
\[ \forall \quad D^{-1}(X) = I \]
then
\[ D^{-1}(X) = E_1(X) = E_2(X) \]
and
\[ X_1 \uplus X_2 \Rightarrow D^{-1}(X_1) \uplus D^{-1}(X_2) \].

**Proof of the Theorem:** Given an error correcting code with additional monotonicity properties on the lattice \((0,1)^k\), if \( d \) denotes the Hamming distance and if \( W \) denotes the weight of a sequence, then
\[ d(Z_1, Z_2) = W(Z_1) + W(Z_2) - 2W(Z_1 \land Z_2) \geq 2s + 1, \quad s \leq \epsilon n. \]

Also
\[ Z_1 \uplus Z_2 = W(Z_1) = W(Z_2) + d(Z_1, Z_2). \]

Consider the chain
\[ 0^k \leq \ldots \leq I^k \theta_0^k \leq \ldots \leq I^k. \]
By the lemma
\[ D^{-1}(I^k) \geq D^{-1}(I^k - 10) \geq \ldots \geq D^{-1}(I^k). \]
Equations (2) and (3) imply
\[ n \geq W[D^{-1}(I^k)] = \sum_{i=0}^{k} d(D^{-1}(I^k - 10^{i}), D^{-1}(I^k - 10^{i+1})) + W(D^{-1}(I^k)) \]
and thus by (1)
\[ n \geq k(2s + 1) + W(D^{-1}(I^k)) \geq k(2s + 1). \]

Q.E.D.

**Observation:** Winograd's proof only uses that \( \varphi \leq D^{-1} \) is monotonic and injective. It does not use the property \( \varphi(a \land b) = \varphi(a) \land \varphi(b). \)

IV. LATTICE CODES

To better understand the coding problem treated, we state it in purely combinatorial terms without any references to computing. Henceforth, the number of codewords \( M \) will be a power of 2: \( M = 2^k \).

Recall that an \( (M, n, r) \)-error correcting code is a set of words
\[ \{ u_1, \ldots, u_M \} \subset \{0,1\}^n \]
with
\[ d(u_i, u_j) \geq 2s + 1, \quad \text{for } i \neq j. \]

An \((M, n, \lambda_{\text{max}})\)-code (resp. \((M, n, \lambda_{\text{ry}})\)-code) for the BSC with the transmission matrix
\[ w = \begin{pmatrix} 1 - \epsilon & \epsilon \\ \epsilon & 1 - \epsilon \end{pmatrix} \]
is the set of pairs \( \{(v_i, D_i) : 1 \leq i \leq M\} \), where \( D_i \cap D_j = \phi \) \( (i \neq j) \), \( v_i \in \{0,1\}^n \), \( D_i \subset \{0,1\}^n \), and
\[ \max w(D_i^c | v_i) \leq \lambda_{\text{max}}, \quad \left( \text{resp. } \frac{1}{M} \sum_{i=1}^{M} w(D_i^c | v_i) \leq \lambda_{\text{ry}} \right). \]

Motivated by the computing problem in the presence of noise as described earlier, Elias [3] considered the logical operation "\( \wedge \)" for \( f \) and \( F \). In this case the codewords \( \{v_1, \ldots, v_M\} \) carry an additional algebraic structure: for any group under modulo 2 componentwise addition or, equivalently, a subspace of \( GF(2)^k \). Moreover, he proved that those group (or linear) codes achieve the capacity of the BSC. Replacing "\( \wedge \)" by other logical operations, algebraic conditions are imposed on the codes.

Generally, we define algebraic codes \( \lambda_{\wedge, \text{ry}} \) by requiring that \( \{ u_1, \ldots, u_M \} \) (resp. \( \{ v_1, \ldots, v_M \} \) ) be parametrized by
\[ \{ u_1, \ldots, u_M \} = \{ \varphi(z) : z \in \{0,1\}^k \} \]
\[ \{ v_1, \ldots, v_M \} = \{ \varphi(z) : z \in \{0,1\}^k \} \].

In this notation linear codes are obtained by an isomorphic vector space embedding of \( GF(2)^k \) into \( GF(2)^n \).

Motivated by Winograd's theorem, we are concerned here with maps \( \varphi \), which preserve lattice properties of \( \{0,1\}^k \), such as monotonicity
\[ a \leq b \Rightarrow \varphi(a) \leq \varphi(b) \]
or preservation of the min-operation "\( \wedge \)"
\[ \varphi(a \wedge b) = \varphi(a) \wedge \varphi(b), \]
\[ a \wedge b = (a_1 \wedge b_1, \ldots, a_k \wedge b_k) \ldots \]
We adopt the following notation: For a code length \( M \) and a block length \( n \)
\[ R = \frac{\log M}{n}, \quad \frac{k}{n} \]
is the rate of the code. For a specified class \( \Phi \) of maps, we define the optimal rates
\[ r^\Phi_n(\epsilon) = \max \left\{ \frac{\log M}{n} : \exists (M, n, r) \right\} \]
for some \( \varphi \in \Phi \) and \( \epsilon = \epsilon_n \)
\[ R^\Phi_n(\lambda_{\text{max}}) = \max \left\{ \frac{\log M}{n} : \exists (M, n, \lambda_{\text{max}}, \varphi) \right\} \]
for some \( \varphi \in \Phi \)
\[ R^\Phi_n(\lambda_{\text{ry}}) = \max \left\{ \frac{\log M}{n} : \exists (M, n, \lambda_{\text{ry}}, \varphi) \right\} \]
for some \( \varphi \in \Phi \).

The class of all \( \psi : \{0,1\}^k \to \{0,1\}^n \) for some \( k,n \) that are injective and \( \wedge \)-preserving is denoted by \( \Psi \). In this notation Winograd's theorem can be considered as follows. For \( 0 < \epsilon < 1 \)
\[ r^\Psi_n(\epsilon) \leq (2\epsilon)^{-1} - 1 \to 0 \quad (n \to \infty). \]
V. A LOWER BOUND ON $R_0^\lambda(\lambda_{\max})$

Theorem 1: $R_0^\lambda(\lambda_{\max}) \geq d(\epsilon, \lambda) \cdot (\log n)^{-1}$ for a suitable $d(\epsilon, \lambda) > 0$.

Proof: Choose $b \sim k < b$ with $b$ to be specified later. For $x \in \{0, 1\}$, let $(x)^b \equiv (x, x, \ldots, x)$ be of length $b$ and define $\varphi$: $(0, 1)^b \to (0, 1)^n$ as

$$\varphi(x^b) = \varphi(x_1, \ldots, x_n) = (x_1)^b, \ldots, (x_n)^b).$$

(14)

Obviously, $\varphi$ is injective and $\lambda \vee \lambda' \geq \varphi$-preserving. Thus, particularly $\varphi \in \Psi$. For the codewords $\{\varphi(x^b); x \in \{0, 1\}^b\}$, define decoding sets $D_\lambda$ by maximum likelihood decoding with respect to the BSC (declare an error in case of ties). By symmetry the individual error probabilities are all equal and thus $\lambda_{\max} = \lambda_{\max}^{\lambda_{\max}}$. We calculate now $\lambda_{\max}$. First observe that there are exactly $n!$ codewords that differ from a fixed codeword $\varphi(x^b)$ in exactly $l$ blocks. The two-codeword error probability of $\varphi(x^b)$ and such a codeword is less than $e^{-\epsilon/l}$ for a suitable constant $c > 0$. Therefore

$$\lambda_{\max} \leq \sum_{l=1}^{k} \binom{k}{l} e^{-\epsilon/l} \leq \sum_{l=1}^{k} e^{-\epsilon/l} = k e^{-\epsilon/l} \leq \lambda, \quad \text{if} \quad k e^{-\epsilon/l} < 1.$$

(15)

This condition holds for any $b$ with

$$1 + c(\epsilon)^{-1} \log k - \frac{\lambda}{2} \geq b \geq c(\epsilon)^{-1} \log k - \frac{\lambda}{2}$$

and therefore

$$R_0^\lambda(\lambda) \geq \frac{k}{n} - \frac{1}{b} \geq \left(1 - c(\epsilon)^{-1} \log k + c(\epsilon)^{-1} \log k \right)^{-1}
\geq \frac{c(\epsilon)}{2 \log k}, \quad \text{for} \quad k \geq k_\epsilon(\epsilon, \lambda)$$

which gives the result, because $n \geq k$.

VI. WEAK CONVERSE VIA CHAINS

One readily verifies

$$\varphi \wedge \varphi \text{-preserving} \implies \varphi \text{monotonic}.$$

Thus $\Psi \subset \mathbb{M}$, the class of injective, monotonic maps. Actually Winograd’s proof, which is based on the properties of a chain of codewords, uses monotonicity (in the form $x_1 \geq x_2 \Rightarrow D^{-1}(x_1) \geq D^{-1}(x_2)$ of the Lemma) rather than the $\wedge$-preserving property. Here we analyze how far this argument holds. Later we derive sharper results by looking at antichains.

Theorem 2: (Weak converse for maximum error.) For any null sequence $(\lambda_d)_{d=1}^{\infty}$ we have $\lim_{d \to \infty} R_0^\lambda(\lambda_d) = 0$.

Proof: Consider any chain of length $k$ in $(0, 1)^b$, such as $e_1 \equiv e_1, e_1 \equiv e_2, e_1 \equiv e_3, \ldots, e_1 \equiv e_2 \equiv e_3 \equiv \ldots \equiv e_k$

where $e_i = (0, 0, 0, 1, 0, 0, 0)$ with a one in the $i$th position. Then $\varphi(e_1) \leq \varphi(e_t) \leq \ldots \leq \varphi(e_1 \equiv \ldots \equiv e_k)$, and therefore there exists $c_1, \ldots, c_t \in \{0, 1\}^n$ with $c_i \wedge c_j = 0 = (0, \ldots, 0), \quad i \neq j$

and

$$\varphi(e_1 \equiv \ldots \equiv e_t) = c_1 \equiv c_2 \equiv \ldots \equiv c_t, \quad i = 1, \ldots, k.$$

(17)

For two successive codewords the two-codeword error probabilities satisfy for a suitable constant $f(\epsilon) > 0$

$$\lambda_n \geq \max(\lambda(\varphi(e_1 \equiv \ldots \equiv e_t), \lambda(\varphi(e_1 \equiv \ldots \equiv e_{t+1})))
\geq e^{-f(\epsilon)l_{t+1}}.$$

(18)

Therefore,

$$\lambda_{t+1} \geq -\frac{1}{f(\epsilon) \log \lambda_n}, \quad n \geq \sum_{t=1}^{k} c_t \geq -\frac{k}{f(\epsilon) \lambda_n},$$

and

$$\frac{k}{n} \leq -f(\epsilon) \frac{\log \lambda_n}{n} \to 0, \quad (n \to \infty).$$

Q.E.D.

Next we establish a somewhat weaker result for average errors.

Theorem 3: ("Very" weak converse for average errors.) For any null sequence $(\lambda_d)_{d=1}^{\infty}$ with $0 < \lambda_d \leq e^{-\delta n}, \delta > 0, d \in \mathbb{N}$

$$\lim_{d \to \infty} R_d^\lambda(\lambda_d) = 0.$$

To apply the previous argument, we must find a subcode of small maximal error probability that contains a chain of sufficient length.

In the multiuser information theory [8], the attempt to extract a suitable maximal error code from an average error code led to the combinatorial problem of Zarankiewicz. The situation here is similar. We are led to another combinatorial problem that was solved by Erdős [9] (Theorem 2.3 in [10]). For arbitrary $\mathcal{B} \subset \{0, 1\}^k, |\mathcal{B}| = B$, what is the guaranteed length $L(B, k)$ of the longest chain in $\mathcal{B}$?

Define $N_k$ by

$$N_k = \max \text{integer with } \left\{ \begin{array}{l} n_k \geq 2 \left( \frac{k}{2} - s \right) \geq 2 \left( \frac{k}{2} - s \right) \leq B, \quad k \text{ is even} \quad (20) \end{array} \right.$$

$$\left\{ \begin{array}{l} n_k \geq 2 \left( \frac{k}{2} + s \right) \leq B, \quad k \text{ is odd.} \quad (21) \end{array} \right.$$

Erdős proved

$$L(B, k) \geq \left\{ \begin{array}{l} 2N_k + 1, \quad \text{if} \ k \text{ is even} \quad (22) \end{array} \right.$$

$$\left\{ \begin{array}{l} 2N_k, \quad \text{if} \ k \text{ is odd.} \quad (23) \end{array} \right.$$

Proof: Consider the subcode

$$\varphi = \{ \varphi(x^b); x^b \in \{0, 1\}^k \}$$

and

$$w(D_{\varphi}(\varphi(x^b)) \leq 2\lambda_n)$$

which by a pigeonhole argument satisfies

$$|\mathcal{B}| \geq \frac{1}{2} \cdot 2^k.$$
of a chain \( \mathcal{Q}_0 \subset \mathcal{Q} \) with
\[
|\mathcal{Q}_0| \geq \text{const. } \sqrt{\varepsilon}.
\] (23)
The argument given in the proof of Theorem 2 can now be applied to the chain \( \mathcal{Q}_0 \). The corresponding quantities \( c_i, \cdots, c_{\text{const. } \sqrt{\varepsilon}} \) satisfy
\[
e^{-\varepsilon k} \geq e^{-f(\varepsilon)}.
\]
Thus,
\[
c_i \geq \frac{\varepsilon k}{f(\varepsilon)}
\]
\[
n \geq \sum_{i=1}^{k} c_i \geq \text{const. } \sqrt{\varepsilon} \frac{\varepsilon k}{f(\varepsilon)}
\]
and finally
\[
\frac{k}{n} \leq \text{const. } k^{-1/2}.
\]
Q.E.D.

**Remark 1:** Of course, the proof still works for
\[
\lambda_0 \leq e^{-\varepsilon \log_{1/\varepsilon}}, \quad \eta > 0.
\]

**Remark 2:** Notice that we have not proved the strong converse [6] that says here
\[
\lim_{n \to \infty} R_n^*(\lambda) = 0 \quad \text{resp.} \quad \lim_{n \to \infty} R_n^*(\lambda) = 0
\]
for every constant \( \lambda \in (0, 1) \). (24)

In contrast to many situations in coding theory, where the question whether both the weak and strong converse hold is often just of academic interest, the strong converse is of great significance for computing problems. If it does not hold in a certain situation, then computing in the presence of noise is possible at a positive rate for certain error probabilities. Unfortunately the strong converse does hold, and thus the desired phenomenon does not occur for the class \( \mathcal{Q} \). For this class the sharper result can be derived by looking at antichains.

**Remark 3:** As an instructive exercise in abstract coding theory [6], we propose a problem does (24) hold for maximal (or even average) errors?

**VII. STRONG CONVERSE VIA ANTICHAINS**

**Theorem 4:** (Strong converse for maximal error)
\[
\lim_{n \to \infty} R_n^*(\lambda) = 0, \quad \lambda \in (0, 1).
\]

More precisely,
\[
d_i(\varepsilon, \lambda) (\log n)^{-1} \leq R_n^*(\lambda) \leq d_i(\varepsilon, \lambda) (\log n)^{-1}
\]
for suitable constants \( d_1, d_2, \text{and } n \geq 2 \).

**Proof:**
\( a) \) Suppose that \( \Psi(0, \cdots, 0) \) has a one in some components, then because of monotonicity all codewords \( \Psi(x^n) \) have a one in those components. They therefore add nothing to the error performance and just decrease the rate. Thus, without loss of generality (w.l.o.g.) suppose that
\[
\Psi(0, \cdots, 0) = (0, \cdots, 0) \in (0, 1)^n.
\] (25)

By the previous argument we can assume
\[
\bigcup_{i=1}^{k} S_i = \{1, 2, \cdots, n\}.
\] (26)

Thus, for \( c_i = |S_i| \)
\[
\sum_{i=1}^{k} c_i = n.
\] (27)

We will derive the desired bound on the rate by analyzing the error performance of the antichain only.
\( c) \) Next, we modify this antichain so that the new supports have all equal cardinalities. Define \( \mathcal{Q} = \sum_{i=1}^{k} c_i / k \). Then \( |\{i: c_i > 2\mathcal{Q}\}| 2\mathcal{Q} \leq k \mathcal{Q} = n \) and hence \( |\{i: c_i > 2\mathcal{Q}\}| \leq (n/2\mathcal{Q}) - k/2 \).

For the sake of convenience, set \( m = k/2 \) and \( d = [2\mathcal{Q}] \).

Thus we have a subantichain \( \{\Psi(a_i): 1 \leq i \leq m\} \) with \( c_i \leq d \). To simplify the calculation of the error probability, extend all \( c_i \) to \( d \), disregarding the increase in the total length or equivalently the loss in rate. An antichain, which each codeword has by symmetry, is obtained for the same error performance in strict (disregarding ties) maximum likelihood decoding. We upper bound the probability of correct decoding for one codeword by a rough estimate.

\( d) \) For the strict maximum likelihood decoding code \( \{\Psi(a_i), D_{\Psi(a_i)}\}: 1 \leq i \leq m \)
\[
D_{\Psi(a_i)} = \{ \Psi(y^n) \neq \Psi(a_i), \quad \text{for all } j \neq i \}
\] (28)
because \( y^n \neq \Psi(a_i) \) implies \( w(y^n|\Psi(a_i)) \geq w(y^n|\Psi(a_i)) \). Obviously, from (28)
\[
w(D_{\Psi(a_i)}|\Psi(a_i)) \leq (1 - (1 - \varepsilon) d)^{m-1}
\] (29)
and necessarily with \( \eta \equiv 1 - \varepsilon \)
\[
(1 - \eta)^{m-1} \geq 1 - \lambda.
\] (30)
This gives a lower bound on \( d \), and thus the desired upper bound on the rate is
\[
R = R/n - 1/n \leq 2 \mathcal{Q} \leq 2 \mathcal{Q} / d,
\]
since \( d \leq 2\mathcal{Q} \). From (20)
\[
\log(1 - \eta) \geq -\log(1 - \lambda)
\]
and therefore necessarily from \( \log(1 - x) \leq -x \),
\[
-\eta \geq -\log(1 - \lambda)
\]
\[
d \geq \left[\log \left(1 - \log(1 - \lambda)\right)\right]^{1/\log(1 - \lambda)}
\]
Thus
\[
R \leq \frac{2}{d} \leq 2 \log \frac{1}{\log(1 - \lambda) - 1} - \log(1 - \lambda)
\]
Since \( \eta = 1 - \varepsilon, m = k/2, \) a constant \( \rho(\lambda, \varepsilon) \) exists for which
\[
R = \frac{R}{n} \leq \rho(\lambda, \varepsilon)(1) \left(\log k\right)^{-1}, \quad k \geq 4.
\] (31)

\( e) \) Finally, this bound is expressed in terms of \( n \). Since \( R \leq 1 \), substitution of \( R_n \) for \( k \) in (31) yields
\[
R \leq \rho \log R + \log n.
\] (32)
Suppose now that for every $k > 0$ $R \geq k/\log n$ for $n$ large, then
\[
\frac{k}{\log n} \leq \frac{\rho}{\log k - \log \log n + \log n}
\]
or
\[
\log k - \log \log n + \log n \leq \frac{2k}{\log n},
\]
a contradiction. Thus, $R_k^*(\lambda) = O(1/\log n)$ and by Theorem 1 this bound is best within a constant for the first-order term.

**Theorem 5:** (Strong converse for average error)

\[
\lim_{n \to \infty} R_k^*(\lambda) = 0, \quad \lambda \in (0, 1).
\]

Actually,
\[
\tilde{d}_k(\epsilon, \lambda)(\log n)^{-1} \leq R_k^*(\lambda) \leq \tilde{d}_k(\epsilon, \lambda)(\log n)^{-1}
\]
for suitable constants $d_1, d_2$, and $n \geq 2$.

**Proof:**

a) *Auxiliary combinatorial lemma:* Paralleling the proof of Theorem 3, we find a sufficiently long maximal error subcode with $\lambda_{\text{max}} = (1 + \delta)\lambda$ that now has the structure of an antichain and an additional "disjointness property" like the one used in the proof of Theorem 4. For this purpose, we first derive an auxiliary combinatorial result.

Let $\mathcal{G}$ be a directed graph with vertex set $\mathcal{V}$. For $v \in \mathcal{V}$ denote by $\mathcal{F}(v)$ (resp. $\mathcal{E}(v)$) the set of vertices reaching $v$ (resp. reached from $v$) by an arrow. Further, let
\[
I_{\text{max}} \triangleq \max_{v \in \mathcal{V}} |\mathcal{F}(v)|, \quad I \triangleq |\mathcal{V}|^{-1} \sum_{v \in \mathcal{V}} |\mathcal{F}(v)|
\]
denote the maximal and the average in degrees.

**Lemma 1:** Let $\mathcal{V}_1 \cup \mathcal{V}_2$ be a partition of the vertex set of a directed graph $\mathcal{G}$ such that
\[
|\mathcal{V}_1| > |\mathcal{V}|(1 - (1 - \sigma)I_{\text{max}}^{-1}).
\]
Then there exists a $v_0 \in \mathcal{V}$ with
\[
|\mathcal{E}(v_0) \cap \mathcal{V}_1| \geq \sigma I.
\]

**Proof:** Suppose that (34) does not hold. Then
\[
\sum_{v \in \mathcal{V}_1} |\mathcal{F}(v)| = \sum_{v \in \mathcal{V}} |\mathcal{E}(v) \cap \mathcal{V}_1| < |\mathcal{V}|\sigma I,
\]
and therefore
\[
|\mathcal{V}_2|I_{\text{max}} \geq \sum_{v \in \mathcal{V}_2} |\mathcal{F}(v)| > |\mathcal{V}|(1 - \sigma)I.
\]

Thus
\[
|\mathcal{V}_1| \geq |\mathcal{V}|(1 - \sigma)I_{\text{max}}^{-1}
\]

in contradiction to $|\mathcal{V}| = |\mathcal{V}_1| + |\mathcal{V}_2|$ and (33).

b) *Definition of the graph:* The following definitions are motivated by the fact that most words $x^k$ are in the "middle" of the lattice and that we are interested in those with "good" codewords. Write $\lambda(x^k) = \max_{\mathcal{G}(x^k)} |\mathcal{F}(x^k)|$ and consider for $0 < \rho < 1/2$ and $\gamma$ with $(1 + \gamma)\lambda < 1$ the sets
\[
\mathcal{V} = \mathcal{V}(\rho) \triangleq \{ x^k \in (0, 1)^k : |d(x^k, 0) - \frac{1}{2}k | \leq \rho k \}
\]
(35)
\[
\mathcal{V}_1 = \mathcal{V}_1(\gamma, \rho) \triangleq \{ x^k \in \mathcal{V}(\rho) : \lambda(x^k) \leq (1 + \gamma)\lambda \},
\]
(36)
\[
\mathcal{V}(\gamma, \rho) \triangleq \{ x^k \in \mathcal{V}(\rho) : \lambda(x^k) > (1 + \gamma)\lambda \}.
\]
(37)

Now define a directed graph $\mathcal{G}$ with vertex set $\mathcal{V}(\rho)$ by
\[
\nu \to \nu \leftrightarrow \nu \mu \nu \to \nu
\]
where $u, v$ differ in exactly one component.

**c) Application of Lemma 1:** To apply the lemma to the graph $\mathcal{G}$ and the partition $\mathcal{V} = \mathcal{V}_1 \cup \mathcal{V}_2$, we must first estimate $|\mathcal{V}|, |\mathcal{V}_1|, I_{\text{max}}$, and $I$.

It is well-known that
\[
|\mathcal{V}| = |\mathcal{V}(\rho)| \geq (1 - e^{-f(\rho)}k)^{2k} \quad (39)
\]
for a suitable constant $f(\rho) > 0$. Since
\[
\lambda_2 = \sum_{x^k \in (0, 1)^k} \lambda(x^k) \geq \{ \lambda(x^k) = (1 + \gamma)\lambda \}(1 + \gamma)\lambda
\]
we have
\[
[ x^k \in (0, 1)^k : \lambda(x^k) \leq (1 + \gamma)\lambda ] \geq \frac{\gamma}{1 + 2^k}
\]
which together with (39) implies
\[
|\mathcal{V}_1| - |\mathcal{V}(\gamma, \rho)| \geq \left(1 + \frac{1}{2} + e^{-f(\rho)k}\right). \quad (40)
\]

Obviously, from the definitions it follows that
\[
I_{\text{max}} = \left(1 + (1 - \rho)k \right)
\]
and
\[
(1 - \rho)k \leq I \leq (1 + \rho)k. \quad (42)
\]

Actually, $I$ is almost equal to $(1/2)k$.

Next, we ensure condition (33). Choose $0 < \sigma \leq \gamma/4(1 + \gamma)$, then $0 < \sigma \leq 1/4$ and so small that $(1/2 - \rho)/(1/2 + \rho) \geq 1 - \sigma$. Thus
\[
\frac{1}{1 + \gamma} - 2\sigma \geq 2\sigma - \sigma^2
\]
and for $k \geq k_0(\gamma, \rho)$
\[
\frac{1}{1 + \gamma} - e^{-f(\rho)k} \geq 1 - (1 - \sigma)I_{\text{max}}^{-1}.
\]

Therefore
\[
|\mathcal{V}_2| \leq 2^k, \quad (1 - \sigma)I_{\text{max}}^{-1}
\]
and this, $|\mathcal{V}| \leq 2^k$, and (40) imply condition (33).

The lemma guarantees the existence of a $v_0 \in \mathcal{V}$ with
\[
|\mathcal{E}(v_0) \cap \mathcal{V}_1| \geq \sigma I \geq \frac{1}{4} + \frac{1}{4} + \frac{1}{4} k
\]
by the definition of $\sigma$, (42), and $\rho \leq 1/4$.

**d) The desired antichain in $\mathcal{G}(\gamma, \rho)$:** For $k' = k/16(1 + \gamma)$ consider a subset
\[
\{ a_1, \ldots, a_k \} \subset \mathcal{E}(v_0) \cap \mathcal{V}_1 \quad (45)
\]
and define the subcode
\[
\mathcal{G}^* = \{ \mathcal{G}(a_1) : 1 \leq i \leq k' \} \subset \mathcal{G}(\gamma, \rho). \quad (46)
\]
By the definitions of the graph and the $a_i, \mathcal{G}(a_i) \supseteq \mathcal{G}(v_0)$ for all $i$ and $a_i \cap a_j = v_0$ for $i \neq j$. Since $\rho \in \mathcal{Y}$, we have
\[
\mathcal{G}(a_1) \land \mathcal{G}(a_j) = \mathcal{G}(a_1 \land a_j) = \mathcal{G}(v_0). \quad (47)
\]

This means that the supports of the $\mathcal{G}(a_i)$ contain the support of $\mathcal{G}(v_0)$ and are disjoint in its complement. Dropping the component in the support of $\mathcal{G}(v_0)$ leads to a code of the same rate and error performance. This is exactly the maximal error code used in the proof of Theorem 4, and the proof of Theorem 5 can be completed in the same way.
Another Proof of Theorem 5: The preceding proof was based on a rather general idea. Using more of the lattice structure, we can provide a simpler proof.

Define \( \mathcal{F}_r = \{ x^r : x^r \in (0,1)^r : \alpha(x^r,0) = \gamma \} \). From the argument leading to (40), for any \( 0 < \rho < 1/2 \) and \( r \leq (l + I)/2 \), such that

\[
\gamma_x^r \equiv \{ x^r : x^r \in \mathcal{F}_r \}, \lambda_x^r \leq \lambda(1 + \gamma)
\]

\[
|\gamma_x^r| \geq \delta(\lambda_x, \gamma, \rho) \left( \frac{l}{l} \right)
\]

(48)

for a suitable \( \delta \). The following (44) replaces (44). From there the proof can be completed as in d.

Lemma 2: A \( v \in \mathcal{F}_r \) exists such that

\[
|\mathcal{F}(v) \cap \gamma_x^r| \geq \delta(k - (l - 1)).
\]

(44')

Proof: Look at the bipartite graph

\[
\mathcal{F}_r \cup \mathcal{F}_r, \mathcal{F}_r
\]

where

\[
(x^r, y^r) \in \mathcal{F}_r \iff x^r < y^r.
\]

Obviously,

\[
|\mathcal{F}_r| - \left( \frac{k}{l - 1} \right)(k - (l - 1)) = \left( \frac{k}{l} \right)l.
\]

(49)

The number of edges leaving \( \gamma_x^r \) is bigger than \( \delta(\frac{k}{l})l \). Now suppose that for all \( v \in \mathcal{F}_r \)

\[
|\mathcal{F}(v) \cap \gamma_x^r| < \delta(k - (l - 1)).
\]

Then the number of edges to \( \gamma_x^r \) is smaller than

\[
\left( \frac{k}{l - 1} \right) \delta(k - (l - 1)) = \delta(\frac{k}{l})l
\]

which is a contradiction.

Q.E.D.

A Sequence of Upper and Lower Bounds for the Q Function

THOMAS K. PHILIPS AND AHMED SAHRAOUI

Abstract—A sequence of upper and lower bounds for the Q function defined as \( Q(x) = 1/\sqrt{2\pi} \int_x^\infty \exp \left( -y^2/2 \right) dy \) is developed. These bounds are shown to be tighter than those most commonly used.

It has been shown [1], for the Q function defined as

\[
Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty \exp \left( -y^2/2 \right) dy,
\]

that for \( x > 0 \)

\[
\frac{1}{\sqrt{2\pi}} \left( 1 - \frac{1}{x^2} \right) \exp \left( -x^2/2 \right) < Q(x) < \frac{1}{\sqrt{2\pi}} \exp \left( -x^2/2 \right).
\]

Our aim is to develop tighter bounds. Consider rewriting the Q function as

\[
Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty \cdot \exp \left( -y^2/2 \right) dy,
\]

and note that if \( y/x > 1 \), then \( P_0(y) = (1 - (y/x)^2)^\frac{1}{2} \) is an upper bound for \( 1 \) if \( n \) is odd and a lower bound for \( 0 \) if \( n \) is even. Now define

\[
A_n(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty \exp \left( -y^2/2 \right) dy.
\]


