ISSN 2186-6570

An Exposition of a Result in "Conjugate Codes for Secure and Reliable Information Transmission"

Mitsuru Hamada

Quantum Information Science Research Center
Quantum ICT Research Institute
Tamagawa University
6-1-1 Tamagawa-gakuen, Machida, Tokyo 194-8610, Japan

Tamagawa University Quantum ICT Research Institute Bulletin, Vol.7, No.1, 11-16, 2017

Tamagawa University Quantum ICT Research Institute Bulletin
Vol.7 No.1 : 11–16 (2017)

An Exposition of a Result in "Conjugate Codes for Secure and Reliable Information Transmission"

Mitsuru Hamada
Quantum Information Science Research Center
Quantum ICT Research Institute
Tamagawa University
6-1-1 Tamagawa-gakuen, Machida, Tokyo 194-8610, Japan

***Abstract*—An elementary proof of the attainability of random coding exponent with linear codes for additive channels is presented. The result and proof are from Hamada (Proc. ITW, Chendu, China, 2006), and the present material explains the proof in detail for those unfamiliar with elementary calculations on probabilities related to linear codes.**

I. Introduction

These days, 'information-theoretic security' is a term that even ordinary people may recognize as something innovative through the mass media.[1] This article offers expository material for this author's results [1] presented about a decade ago that may be said to precede the boom on information-theoretic security or specifically, wiretap channels (a model of channels subject to eavesdropping) in information theory. More specifically, this material has been prepared for the following reason. Linear codes that could be constructed in polynomial time suggested in [1] were later proved to be asymptotically optimal [10] in that they achieved the secrecy capacities of wiretap channels. The material in this article was prepared when the author wrote [10] since a result in [1] was used in [10] and the detailed proof of the result seemed to be useful in view of the interdisciplinarity of that work. We remark that while in [1], they have been presented as coding-theoretic '(quotient) codes' or something equivalent, the corresponding encoders are emphasized in [10]. As a result, the latter would be much more readable. (Note that classical coding theory mainly treats 'codes' for ordinary channels without countermeasures against eavesdropping, and the coding-theoretic 'code' can be understood as a set associated with an encoder in the following manner. An encoder is a one-to-one mapping from the whole space ${\mathbb{F}_q}^k$ of k-dimensional numerical vectors over a finite field $\mathbb{F}_q$ to the whole space of n-dimensional numerical vectors ${\mathbb{F}_q}^n$, where q is a power of a prime and $k \leq n$. For example, when $q = 2$, $\mathbb{F}_q = \{0, 1\}$ and ${\mathbb{F}_q}^n = \{0, 1\}^n$. Here, the k-dimensional numerical vector represents a message or a string of digits (a sequence of letters) to encode. Then, mathematically speaking, the code is the image of ${\mathbb{F}_q}^k$ under the encoder. The notion of an encoder of codes for ordinary channels extends to an encoder of 'quotient codes' [8] for wiretap channels as in [10].)

In this material, the details of the proof of a result in [1], an article prepared for an invited talk, are presented without assuming any prerequisite knowledge. In fact, when the author prepared the manuscript [2], which includes one illustrative application of the method of concatenating 'conjugate code pairs' devised in [1], [3],[2] the author thought some (or most) proofs are elementary and straightforward, so that they are not needed for those working in our society of information theory. However, in this article, still more details will be presented to increase the accessibility.

We remark that that result and its detailed proof are written so that they can be read without referring to [1]. Specifically, in this material, an elementary proof of the attainability of random coding exponent with linear codes for additive channels is presented. (Of course, many proofs for the attainability of random coding exponent had existed, but the incentive for developing this approach was to design quantum error-correcting codes and codes that can be used in cryptographic protocols. For these purposes, we needed to design codes and decoders under constraints arising from quantum mechanics.)

Thus, this material is supplementary to [1] for those unfamiliar with the elementary approach adopted in [1], but the result treated in this material is compact, classical, and comprehensible without understanding the main issues treated in [1]. This approach is nothing special, but it may be said to be that of the method of types [4], [5], which

[1]The contents of this article are the same as those of the manuscript `arXiv:1001.1806v1`, uploaded on Jan. 12, 2010, except adding this paragraph, the footnotes other than footnote 4 and Refs. [10], [11] (and correcting a few typos) in this version.

[2]Using the term 'concatenate' in this sense may not be readily acceptable for specialists of Forney's well-known concatenated codes. In fact, this usage is fairly different from Forney's, whereas our concatenation here *is* related to Forney's concatenated codes. On the other hand, one would readily agree that the usage of 'concatenate' in Ref. [10] be an extension of Forney's. Regarding [2], the manuscript, which treats an information theoretic issue, was combined with another, which treats a combinatorial or coding-theoretic issue with the conventional coding-theoretic criterion of minimum distance (extended to 'quotient codes' [8]) when it was included in a journal as [3].

requires no prerequisite knowledge, with the very basics of linear codes incorporated.

The aforementioned illustrative application of the method for concatenation is construction of pairs of linear codes (L_1, L_2) with $L_2^{\perp} \subseteq L_1$ ('conjugate code pairs') that achieve a high information rate on the Shannon theoretic criterion. Such a code pair can be viewed as a succinct representation of the corresponding quantum error-correcting code (QECC). The code construction is explicit in the standard sense that the codes are constructible with polynomial complexity. Another (cryptographic) application, which reflects the original motivation of [1], [2] has been presented in [6].[3]

II. Corrections and Remark to [1]

A. Corrections to [1]; Some Apply Also to [2]

1) p. 149, right column, line 14, 'ensemble' should be followed by '(multiset)'
2) p. 150, left column, line -1,

$$a_n|\mathcal{P}_n|^2 d^{-nE_{\mathrm{r}}(W,r)}$$

should read

$$a_n|\mathcal{P}_n|^2 q^{-nE_{\mathrm{r}}(W,r)}$$

3) p. 150, right column, line -9, 'parameter k' should read 'the number k/n'
4) p. 151, left column, line -8, '$(y_1^{(i)} \cdots y_N^{(i)})$' should read '$(y^{(1)} \cdots y^{(N)})$'
5) p. 152, left column, line 1, '$(\bigoplus_{i=1}^t C_1^{(i)}, \bigoplus_{i=1}^t C_2^{(i)})$' should read '$(\bigoplus_{j=1}^t C_1^{(i)}, \bigoplus_{j=1}^t C_2^{(i)})$',
6) p. 152, left column, Eq. (6),

$$M_Q(C) \leq (|\mathcal{P}_n(\mathbb{F}_q)| - 1) q^{-n(1-r_{\mathrm{c}})} A$$

should read

$$M_Q(C_j^{(i)}) \leq (|\mathcal{P}_n(\mathbb{F}_q)| - 1) q^{-n+k_j} |\mathcal{T}_Q^n| A$$

Essentially the same errors as in 1, 2 and 6 exist in Section 4 of [2] (ver. 2), but the contents of Section 4 of [2] are presented below in the corrected form.

B. Remark to [1], [2]

Note that, in [1], [2], an ensemble has been represented as a multiset, which is similar to a usual set but permits duplicated entries.

Now, the author thinks representing an ensemble as an ordered set is more natural, as will be done in the present article.

[3]The efforts to analyze the performance of codes suggested in [1] on classical wiretap channels culminated in the optimality result [10], so that if one was only interested in classical wiretap channels, [6] might have only historical meanings now.

III. Preliminaries

In this section, we fix our notation, and recall some notions to be used. As usual, $\lfloor a \rfloor$ denotes the largest integer a' with $a' \leq a$, and $\lceil a \rceil = -\lfloor -a \rfloor$. An $[n, k]$ linear (error-correcting) code over a finite field $\mathbb{F}_q$, the finite field of q elements, is a k-dimensional subspace of ${\mathbb{F}_q}^n$. The dual of a linear code $C \subseteq {\mathbb{F}_q}^n$ is $\{y \in {\mathbb{F}_q}^n \mid \forall x \in C,\ x \cdot y = 0\}$ and denoted by $C^{\perp}$, where $x \cdot y = xy^{\mathrm{t}}$ with y^{t} being the transpose of y. The zero vector in ${\mathbb{F}_q}^n$ is denoted by 0_n. The $n \times n$ identity (resp. zero) matrix is denoted by I_n (resp. O_n). For integers $i \leq j$, we often use the set $[i, j] \cap \mathbb{Z} = \{i, i+1, \ldots, j\}$, which consists of integers lying in the interval $[a, b] = \{z \in \mathbb{R} \mid a \leq z \leq b\}$.

We denote the type of $x \in {\mathbb{F}_q}^n$ by P_x [4], [5]. This means that the number of appearances of $u \in \mathbb{F}_q$ in $x \in {\mathbb{F}_q}^n$ is $n\mathsf{P}_x(u)$. The set of all types of sequences in ${\mathbb{F}_q}^n$ is denoted by $\mathcal{P}_n(\mathbb{F}_q)$. Given a set $C \subseteq {\mathbb{F}_q}^n$, we put $M_Q(C) = |\{y \in C \mid \mathsf{P}_y = Q\}|$ for types $Q \in \mathcal{P}_n(\mathbb{F}_q)$. The list of numbers $(M_Q(C))_{Q \in \mathcal{P}_n(\mathbb{F}_q)}$ may be called the P-spectrum (or simply, spectrum) of C. For a type Q, we put $\mathcal{T}_Q^n = \{y \in {\mathbb{F}_q}^n \mid \mathsf{P}_y = Q\}$. We denote by $\mathcal{P}(\mathcal{Y})$ the set of all probability distributions on a set $\mathcal{Y}$. The entropy of a probability distribution P on $\mathcal{Y}$ is denoted by $H(P)$, viz., $H(P) = \sum_{y \in \mathcal{Y}} -P(y) \log P(y)$. Throughout, logarithms are to base q.

We follow the convention to denote by P_{X} the probability distribution of a random variable X.

IV. Good Codes in a Balanced Ensemble

A. Balanced Ensemble

We can find good codes in an ensemble if the ensemble is 'balanced' in the following sense. Suppose $\mathsf{S} = \{C^{(i)}\}_{i=1}^N$ is an ensemble (ordered set) of subsets of ${\mathbb{F}_q}^n$. If there exists a constant V such that $|\{i \in [1, N] \cap \mathbb{Z} \mid x \in C^{(i)}\}| = V$ for any word $x \in {\mathbb{F}_q}^n \setminus \{0_n\}$, the ensemble S is said to be *balanced*. (We remark that the 'balancedness' is defined in a different manner in [7] for ensembles of encoders, not codes.)

The first task in [1] was to construct a relatively small balanced ensemble. This result can be found in [1], [2], but it is included in Appendix B. With the method of types, we will show that a large portion of a balanced ensemble consists of good codes. While the goodness of codes should be evaluated by the decoding error probability, it is also desirable to quantify the goodness in such a way that the goodness does not depend on characteristics of channels. In view of this, the following proposition is useful.

The next proposition relates the spectrum of a code with its decoding error probability when it is used on an additive memoryless channel.

Proposition 1: [8, Theorem 4]. Suppose we have an $[n, \kappa]$ linear code C over $\mathbb{F}_q$ such that

$$M_Q(C) \leq a_n q^{\kappa - n} |\mathcal{T}_Q^n|, \quad Q \in \mathcal{P}_n(\mathbb{F}_q) \setminus \{\mathsf{P}_{0_n}\}$$

for some $a_n \geq 1$. Then, its decoding error probability with the minimum entropy syndrome decoding is upper-bounded

by

$$a_n|\mathcal{P}_n(\mathbb{F}_q)|^2 q^{-nE_{\rm r}(W,r)}$$

for any additive channel W of input-output alphabet $\mathbb{F}_q$, where $r = \kappa/n$ and $E_{\rm r}(W,r)$ is the random coding exponent of W defined by

$$E_{\rm r}(W,r) = \min_{Q\in\mathcal{P}(\mathbb{F}_q)} [D(Q||W) + |1 - r - H(Q)|^+].$$

Here, D and H denote the relative entropy and entropy, respectively, and $|x|^+ = \max\{0, x\}$.

For a poof, see Section IV-C. In the simplest case where $q = 2$, the premise of the above proposition reads 'the spectrum of C is approximated by the binomial coefficients $|\mathcal{T}_Q^n|$ up to normalization.'

The following lemma shows a large portion of a balanced ensemble $\{C^{(i)}\}_{i=1}^{N^*}$ is made of good codes (we have applied this fact to ensembles written as $\{C_j^{(i)}\}_{i=1}^{N^*}$ in [1], [2]).

Lemma 1: [1, p. 152, left column]. Assume we have a balanced ensemble $\{C^{(i)}\}_{i=1}^{N^*}$. Let us say an $[n,\kappa]$ code $C^{(i)}$ is A-good if

$$M_Q(C^{(i)}) \le A(|\mathcal{P}_n(\mathbb{F}_q)| - 1)q^{-n(1-\rho)}|\mathcal{T}_Q^n| \qquad (1)$$

for all $Q \in \mathcal{P}_n(\mathbb{F}_q) \setminus \{\mathsf{P}_{0_n}\}$, where $\rho = \kappa/n$. Then, the number of codes that are not $q^{\varepsilon n}$-good in $\{C^{(i)}\}_{i=1}^{N^*}$ is at most

$$z = \lfloor N^* q^{-\varepsilon n} \rfloor. \qquad (2)$$

This lemma will be proved in Section IV-B. Note, owing to Proposition 1, for the $q^{\varepsilon n}$-good codes $C^{(i)}$ in the above lemma, the decoding error probability is upper-bounded by

$$a_n' q^{-n[E_{\rm r}(W,\rho)-\varepsilon]}, \qquad (3)$$

where $a_n' = |\mathcal{P}_n(\mathbb{F}_q)|^3$ is at most polynomial in n.

B. Proof of Lemma 1

A proof of Lemma 1 will be given, though it may be a routine in information theory. We have a lemma.

Lemma 2: Assume S and $\mathcal{W}$ are finite sets, and non-negative numbers $f_w(x)$ are associate with each pair $(x,w) \in \mathsf{S}\times\mathcal{W}$. Denote by $\overline{f}_w$ the average of $f_w(x)$ over S:

$$\overline{f}_w = \frac{1}{|\mathsf{S}|}\sum_{x\in\mathsf{S}} f_w(x).$$

Then, for any $a > 0$, the number of members in S that fail to satisfy the condition

$$\forall w \in \mathcal{W}, \quad f_w(x) \le \overline{f}_w|\mathcal{W}|a$$

is upper-bounded by $a^{-1}|\mathsf{S}|$.

Proof. Let X be a random variable uniformly distributed over S. Then, the probability that X fails to satisfy '$\forall w \in \mathcal{W}, f_w(X) \le \overline{f}_w|\mathcal{W}|a$' is upper-bounded as follows:

$$\begin{aligned}
&\Pr\{\exists w \in \mathcal{W},\ f_w(X) > \overline{f}_w|\mathcal{W}|a\} \\
&\quad\le \sum_w \Pr\{f_w(X) > |\mathcal{W}|\overline{f}_w a\} \\
&\quad\overset{(i)}{=} \sum_{w:\,\overline{f}_w>0} \Pr\{f_w(X) > |\mathcal{W}|\overline{f}_w a\} \\
&\quad\overset{(ii)}{\le} \sum_{w:\,\overline{f}_w>0} (|\mathcal{W}|a)^{-1} \le a^{-1}, \qquad (4)
\end{aligned}$$

where the equality (i) and inequality (ii) follow from the fact that $\overline{f}_w = 0$ implies $f_w(x) = \overline{f}_w|\mathcal{W}|a = 0$ for all $x \in \mathsf{S}$, and Markov's inequality, respectively. Markov's inequality is included at the end of this subsection with a proof. The lemma immediately follows from (4). □

Proof of Lemma 1. From the fact that $\{C^{(i)}\}_{i=1}^{N^*}$ is balanced, it follows

$$\frac{1}{N^*}\sum_{i=1}^{N^*} M_Q(C^{(i)}) = \frac{q^\kappa - 1}{q^n - 1}|\mathcal{T}_Q^n| \le \frac{q^\kappa}{q^n}|\mathcal{T}_Q^n| \qquad (5)$$

for any $Q \in \mathcal{P}_n(\mathbb{F}_q)$, $Q \ne \mathsf{P}_{0_n}$. To see this, let V be the number of appearances of any fixed nonzero word in enumerating codewords in $C^{(i)}$, $i \in [1, N^*]\cap\mathbb{Z}$. Then, we have trivial equalities $V(q^n - 1) = N^*(q^\kappa - 1)$ and

$$\sum_{i=1}^{N^*} M_Q(C^{(i)}) = V|\mathcal{T}_Q^n|$$

for any $Q \in \mathcal{P}_n(\mathbb{F}_q)$, $Q \ne \mathsf{P}_{0_n}$.[4] From these, we readily obtain the equality and hence the inequality in (5). Now Lemma 1 follows upon applying Lemma 2 to $\mathsf{S} = \{(C^{(i)}, i) \mid i \in [1, N^*]\cap\mathbb{Z}\}$, where $f_w((C,i)) = M_Q(C)$, $w = Q$ and $\mathcal{W} = \mathcal{P}_n(\mathbb{F}_q) \setminus \{\mathsf{P}_{0_n}\}$. □

Lemma 3 (Markov's Inequality): For a positive constant A, and a random variable Y that takes non-negative values and has a positive mean μ, we have

$$\Pr\{\mathsf{Y} \ge A\mu\} \le 1/A.$$

Proof. We have $\mu = \sum_w P_{\mathsf{Y}}(y)y \ge \sum_{y:\,y\ge\mu A} P_{\mathsf{Y}}(y)y \ge \sum_{y:\,y\ge\mu A} P_{\mathsf{Y}}(y)\mu A = \mu A\sum_{y:\,y\ge\mu A} P_{\mathsf{Y}}(y) = \mu A\Pr\{\mathsf{Y} \ge A\mu\}$, which implies the lemma. □

C. Proof of Proposition 1

We use the following basic inequality [4], [5], [9]:

$$\sum_{y\in\mathbb{F}_q{}^n:\,\mathsf{P}_y=Q} P^n(y) \le q^{-nD(Q||P)} \qquad (6)$$

for any $P \in \mathcal{P}(\mathbb{F}_q)$. (Recall P^n denotes the product of n copies of P.) The symmetric group on $\{1,\dots,n\}$, which

[4]The relation $V(q^n - 1) = N^*(q^\kappa - 1)$ immediately follows by counting the pairs (x, C) such that $x \in C \setminus \{0_n\}$ and C is a component of $\{C^{(i)}\}_{i=1}^{N^*}$ in two ways, and the other equality follows similarly.

is composed of all permutations on $\{1,\dots,n\}$, is denoted by $\mathcal{S}_n$. We define an action of $\mathcal{S}_n$ on ${\mathbb{F}_q}^n$ by

$$\pi((x_1,\dots,x_n)) = (x_{\pi(1)},\dots,x_{\pi(n)})$$

for any $\pi \in \mathcal{S}_n$ and $(x_1,\dots,x_n) \in {\mathbb{F}_q}^n$, and put

$$\pi(C) = \{\pi(x) \mid x \in C\}, \quad \pi \in \mathcal{S}_n,\ C \subseteq {\mathbb{F}_q}^n.$$

The expectation operation with respect to a random variable X taking values in $\mathcal{X}$ is denoted by E_{X}:

$$\mathsf{E}_{\mathsf{X}} f(\mathsf{X}) = \sum_{x\in\mathcal{X}} P_{\mathsf{X}}(x) f(x)$$

where f is a real-valued function on $\mathcal{X}$.

Lemma 4: Assume a linear code $C \subseteq {\mathbb{F}_q}^n$ satisfies

$$M_Q(C\setminus\{0_n\})/|\mathcal{T}_Q^n| \le a_n q^{-nT}, \qquad Q \in \mathcal{P}_n(\mathbb{F}_q)$$

with some real numbers $a_n \ge 1$ and T. Let J be a set of coset representatives for ${\mathbb{F}_q}^n/C$ such that each coset $D \in {\mathbb{F}_q}^n/C$ has a representative that belongs to J and that attains the minimum of $H(\mathsf{P}_x)$, $x \in D$ (the resulting decoding is called minimum entropy decoding). Then, we have for any $P_n \in \mathcal{P}({\mathbb{F}_q}^n)$,

$$\mathsf{E}_{\boldsymbol{\pi}} P_n(\boldsymbol{\pi}(J)^{\mathrm{c}}) \le a_n |\mathcal{P}_n(\mathbb{F}_q)| \sum_{Q\in\mathcal{P}_n(\mathbb{F}_q)} P_n(\mathcal{T}_Q^n) q^{-n|T-H(Q)|^+}$$

where c denotes complement, $|t|^+ = \max\{t,0\}$, and the random variable $\boldsymbol{\pi}$ is uniformly distributed over $\mathcal{S}_n$.

Corollary 1: Assume for a linear code $C \subseteq {\mathbb{F}_q}^n$, $M_Q(C\setminus\{0_n\})$ is bounded as in Lemma 4. Then, with J as in the lemma, we have for any $P \in \mathcal{P}(\mathbb{F}_q)$,

$$P^n(J^{\mathrm{c}}) \le a_n |\mathcal{P}_n(\mathbb{F}_q)|^2 q^{-nE(P,T)}$$

where

$$E(P,T) = \min_{Q\in\mathcal{P}_n(\mathbb{F}_q)} [D(Q||P) + |T-H(Q)|^+].$$

A proof of Lemma 4 is given in the next subsection.

Proof of Corollary 1. Clearly, $\mathsf{E}_{\boldsymbol{\pi}} P^n(\boldsymbol{\pi}(J)^{\mathrm{c}}) = P^n(J^{\mathrm{c}})$. Then, inserting the estimate of $P^n(\mathcal{T}_Q^n)$ in (6) into the bound on $\mathsf{E}_{\boldsymbol{\pi}} P^n(\boldsymbol{\pi}(J)^{\mathrm{c}})$ in the lemma, we have

$$P^n(J^{\mathrm{c}}) \le a_n |\mathcal{P}_n(\mathbb{F}_q)| \sum_{Q\in\mathcal{P}_n(\mathbb{F}_q)} q^{-n[D(Q||P)+|T-H(Q)|^+]}$$

and hence, the corollary.

Putting $T = 1-\kappa/n$ in this corollary, we readily obtain the proposition.

D. Proof of Lemma 4

In the proof, $\mathcal{P}_n(\mathbb{F}_q)$ is abbreviated as $\mathcal{P}_n$. We will show that $G = \mathsf{E}_{\boldsymbol{\pi}} P_n(\boldsymbol{\pi}(J)^{\mathrm{c}})$ is bounded above by the claimed quantity.

Imagine we list up all words in $\pi(C\setminus\{0_n\})$ for all $\pi \in \mathcal{S}_n$ permitting duplication. Clearly, the number of appearances of any fixed word $y \in {\mathbb{F}_q}^n$ in the list only depends on its type $\mathsf{P}_y \in \mathcal{P}_n$. Namely, for any $Q \in \mathcal{P}_n$, there exists a constant, say L_Q, such that

$$|\{\pi \in \mathcal{S}_n \mid y \in \pi(C\setminus\{0_n\})\}| = L_Q \tag{7}$$

for any word y with $\mathsf{P}_y = Q$. Then, counting the number of words of a fixed type Q in the list in two ways, we have $|\mathcal{T}_Q^n| L_Q = |\mathcal{S}_n| M_Q(C\setminus\{0_n\})$. Hence, for any type $Q \in \mathcal{P}_n(\mathbb{F}_q)$

$$\frac{L_Q}{|\mathcal{S}_n|} = \frac{M_Q(C\setminus\{0_n\})}{|\mathcal{T}_Q^n|} \le a_n q^{-nT} \tag{8}$$

by assumption. From (7) and (8), we have

$$\frac{|\mathsf{A}_y(C\setminus\{0_n\})|}{|\mathcal{S}_n|} \le a_n q^{-nT} \tag{9}$$

for any $y \in {\mathbb{F}_q}^n$, where

$$\mathsf{A}_y(C\setminus\{0_n\}) = \big\{\pi \in \mathcal{S}_n \mid y \in \pi(C\setminus\{0_n\})\big\}.$$

Then, we have

$$\begin{aligned} G &= \frac{1}{|\mathcal{S}_n|} \sum_{\pi\in\mathcal{S}_n} \sum_{x\notin J} P_n(x) \\ &= \sum_{x\in{\mathbb{F}_q}^n} P_n(x) \frac{|\{\pi \in \mathcal{S}_n \mid x \notin J\}|}{|\mathcal{S}_n|}. \end{aligned} \tag{10}$$

Since $x \notin J$ occurs only if there exists a word $u \in {\mathbb{F}_q}^n$ such that $H(\mathsf{P}_u) \le H(\mathsf{P}_x)$ and $u - x \in \pi(C\setminus\{0_n\})$ from the design of J specified above (minimum entropy decoding), it follows

$$\begin{aligned} &|\{\pi \in \mathcal{S}_n \mid x \notin J\}|/|\mathcal{S}_n| \\ &\quad\le \sum_{u\in{\mathbb{F}_q}^n:\, H(\mathsf{P}_u)\le H(\mathsf{P}_x)} |\mathsf{A}_{u-x}(C\setminus\{0_n\})|/|\mathcal{S}_n| \\ &\quad\le \sum_{u\in{\mathbb{F}_q}^n:\, H(\mathsf{P}_u)\le H(\mathsf{P}_x)} a_n q^{-nT} \\ &\quad= \sum_{Q'\in\mathcal{P}_n:\, H(Q')\le H(\mathsf{P}_x)} a_n |\mathcal{T}_{Q'}^n| q^{-nT} \\ &\quad\le \sum_{Q'\in\mathcal{P}_n:\, H(Q')\le H(\mathsf{P}_x)} a_n q^{nH(Q')-nT} \end{aligned} \tag{11}$$

where we have used (9) for the second inequality, and another well-known inequality [4], [5], [9]

$$\forall Q \in \mathcal{P}_n(\mathbb{F}_q), \quad |\mathcal{T}_Q^n| \le q^{nH(Q)} \tag{12}$$

for the last inequality. Then, using the inequalities $\min\{at,1\} \le a\min\{t,1\}$ and $\min\{s+t,1\} \le \min\{s,1\}+\min\{t,1\}$ for $a \ge 1, s,t \ge 0$, we can proceed from (10) as follows, which completes the proof:

$$\begin{aligned} &G \\ &\le \sum_{x\in{\mathbb{F}_q}^n} P_n(x) \min\Big\{ \sum_{Q'\in\mathcal{P}_n:\, H(Q')\le H(\mathsf{P}_x)} a_n q^{nH(Q')-nT},\ 1 \Big\} \\ &\le a_n \sum_{Q\in\mathcal{P}_n} P_n(\mathcal{T}_Q^n) \min\Big\{ \sum_{Q'\in\mathcal{P}_n:\, H(Q')\le H(Q)} q^{nH(Q')-nT}, 1 \Big\} \\ &\le a_n \sum_{Q\in\mathcal{P}_n} P_n(\mathcal{T}_Q^n) \sum_{Q'\in\mathcal{P}_n:\, H(Q')\le H(Q)} \min\{q^{-n[T-H(Q')]},\ 1\} \\ &\le a_n |\mathcal{P}_n| \sum_{Q\in\mathcal{P}_n} P_n(\mathcal{T}_Q^n) \max_{Q'\in\mathcal{P}(\mathbb{F}_q):\, H(Q')\le H(Q)} q^{-n|T-H(Q')|^+} \\ &= a_n |\mathcal{P}_n| \sum_{Q\in\mathcal{P}_n} P_n(\mathcal{T}_Q^n) q^{-n|T-H(Q)|^+}. \end{aligned}$$

V. Concluding Remarks

In [1], [3] (or [2]), quantum-mechanically compatible pairs of linear codes that are constructible with polynomial complexity were presented. The Calderbank-Shor-Steane quantum codes corresponding to the constructed pairs achieve the so-called Shannon rate. The most novel result among these would be the method for 'concatenating' compatible (conjugate) code pairs, which have been published in [3].

The present material was prepared for explaining the results not included in [3] for those unfamiliar with the elementary combinatorial approach (the method of types with the very basics of linear codes incorporated).

This material might be included somewhere else (possibly in some other context).[5]

Acknowledgments

This work was supported by JSPS KAKENHI Grant number JP26247016.

Appendix

A. Compatible (Conjugate) Code Pairs [1]

Consider a pair of linear codes (C_1, C_2) satisfying

$$C_2^{\perp} \subseteq C_1, \tag{13}$$

which condition is equivalent to $C_1^{\perp} \subseteq C_2$. The following question arises from an issue on quantum error correction: How good both C_1 and C_2 can be under the constraint (13)? This is the subject treated in [1], [3], [2].

We have named a pair (C_1, C_2) with (13) a conjugate code pair in [1]. In what follows, we will use a 'compatible code pair' in place of 'conjugate code pair.'

B. Code Ensemble Based on Extension Field [1]

The companion matrix of a polynomial $f(x) = x^n - f_{n-1}x^{n-1} - \cdots - f_1 x - f_0$, which is monic (i.e., of which the leading term has coefficient 1), over $\mathbb{F}_q$ is defined to be

$$T = \begin{bmatrix} 0_{n-1} & f_0 \\ & f_1 \\ I_{n-1} & \vdots \\ & f_{n-1} \end{bmatrix}.$$

Let T be the companion matrix, or its transpose, of a monic primitive polynomial of degree n over $\mathbb{F}_q$. Given an $n \times n$ matrix M, let $M|^m$ (resp. $M|_m$) denote the $m \times n$ submatrix of M that consists of the first (resp. last) m rows of M. We put $C_1^{(i)} = \{xT^i|^{k_1} \mid x \in {\mathbb{F}_q}^{k_1}\}$ and $C_2^{(i)} = \{x(T^{-i})^{\mathrm{t}}|_{k_2} \mid x \in {\mathbb{F}_q}^{k_2}\}$ for $i = 1, 2, \ldots$, where M^{t} denotes the transpose of M. Then, setting

$$\mathsf{B} = \mathsf{B}_T = \{(C_1^{(i)}, C_2^{(i)})\}_{i=1}^{q^n-1}, \tag{14}$$

we have the next lemma.

[5]When the author wrote this comment, he had in mind the context of wiretap channels [10], [11], described in Section I, as such a context.

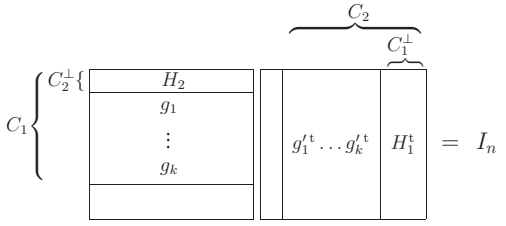

Fig. 1. A basic structure of an $[[n, k]]$ compatible code pair.

Lemma 5: [1, Lemma 1]. Let T be the companion matrix of a monic primitive polynomial of degree n over $\mathbb{F}_q$. For integers k_1, k_2 with $0 \le n - k_2 \le k_1 \le n$ and $\mathsf{B}_T = \{(C_1^{(i)}, C_2^{(i)})\}_{i=1}^{q^n-1}$ constructed as above, any $(C_1^{(i)}, C_2^{(i)})$ is a compatible code pair, and both $\{C_1^{(i)}\}_{i=1}^{q^n-1}$ and $\{C_2^{(i)}\}_{i=1}^{q^n-1}$ are balanced.

Remark. It is known (and proved in a self-contained manner in [3, Sections VII]) that the matrix T has the following property, which are used in the proof of Lemma 5 below: The set $\{O_n, I_n, T, \ldots, T^{q^n-2}\}$ is isomorphic to $\mathbb{F}_{q^n}$ as a field. □

Proof of Lemma 5 [1]. The condition (13) is fulfilled since $T^i T^{-i} = I_n$ implies that the $C_2^{(i)\perp}$ is spanned by the first $n - k_2$ rows of T^i. (This is easily seen if we divide the two matrices on the left-hand side of $T^i T^{-i} = I_n$ into submatrices as in Figure 1.)

We can write $C_1^{(i)} = \{yT^i \mid y \in {\mathbb{F}_q}^n, \mathsf{supp}\, y \subseteq [1, k_1] \cap \mathbb{Z}\}$, where $\mathsf{supp}\,(y_1, \ldots, y_n) = \{i \mid y_i \neq 0\}$. Imagine we list up all codewords in $C_1^{(i)}$ permitting duplication. Specifically, we list up all yT^i as y and i vary over the range $\{y \mid y \in {\mathbb{F}_q}^n, \mathsf{supp}\, y \subseteq [1, k_1] \cap \mathbb{Z}\}$ and over $[1, q^n - 1] \cap \mathbb{Z}$, respectively.

With $y \in {\mathbb{F}_q}^n \setminus \{0\}$ fixed, yT^i, $i \in [1, q^n - 1] \cap \mathbb{Z}$, are all distinct since $T^i \neq T^j$ implies $yT^i - yT^j = yT^l$ for some l and yT^l is not zero. Hence, any nonzero fixed word in ${\mathbb{F}_q}^n$ appears exactly $q^{k_1} - 1$ times in listing yT^i as above. Namely, the ensemble $\{C_1^{(i)}\}_{i=1}^{q^n-1}$ is balanced. Using $(T^{-i})^{\mathrm{t}}$ in place of T^i, we see the ensemble $\{C_2^{(i)}\}_{i=1}^{q^n-1}$ is also balanced, completing the proof. □

Lemmas 1 and 5 show the existence of a compatible code pair having exponentially decreasing decoding error probabilities in B.

References

[1] M. Hamada, "Conjugate codes for secure and reliable information transmission," *Proc. IEEE Information Theory Workshop*, Chengdu, China, pp. 149–153, Oct. 2006.

[2] M. Hamada, "Constructive conjugate codes for quantum error correction and cryptography," 2007. E-Print arXiv:cs/0703141v2 (cs.IT).

[3] M. Hamada, "Concatenated quantum codes constructible in polynomial time: Efficient decoding and error correction," *IEEE Trans. Information Theory*, vol. 54, pp. 5689–5704, Dec. 2008.

[4] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. NY: Academic, 1981.

[5] I. Csiszár, "The method of types," *IEEE Trans. Information Theory*, vol. IT-44, pp. 2505–2523, Oct. 1998.
[6] M. Hamada, "Algebraic and quantum theoretical approach to coding on wiretap channels," *Proc. International Symposium on Communication, Control and Signal Processing*, Malta, pp. 520–525, Mar. 2008.
[7] P. Delsarte and P. Piret, "Algebraic construction of Shannon codes for regular channels," *IEEE Trans. Information Theory*, vol. 28, pp. 593–599, July 1982.
[8] M. Hamada, "Qutoient codes and their reliability," *IPSJ Digital Courier*, vol. 1, pp. 450–460, Oct. 2005. Available at `http://doi.org/10.2197/ipsjdc.1.450`. Also appeared in *IPSJ Journal*, vol. 46, pp. 2428–2438, no. 10, Oct. 2005.
[9] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. NY: Wiley, 1991.
[10] M. Hamada, "Security of concatenated encoders for wiretap channels," *Proc. 2010 IEEE International Symposium on Information Theory (ISIT)*, pp. 2558–2562, Austin, USA, June 2010.
[11] M. Hamada, "Results on constructibility of channel codes," *Proc. 6th Asian-European Workshop on Information Theory*, pp. 31–40, Ishigaki, Japan, Oct. 2010.