On Multiuser Write-Efficient Memories

Rudolf Ahlswede and Zhen Zhang

***Abstract*—Continuing our earlier work on write-efficient memories (WEM), we introduce new models, where several persons use the same storage device. At any time instant, exactly one of a prescribed set of users has access to the memory, but there is no protocol which determines the moving order. Among the constraints we analyze, the most interesting one is a complete privacy protection. While a user stores new data, he has to guarantee that those of the others do not get distorted. This leads to fascinating new coding problems. We provide several code constructions, as well as abstract performance bounds.**

***Index Terms*—Multiuser memories, WEM, WUM, privacy constraints, code constructions, identification.**

I. Introduction: Multiuser Memories with Constraints on Privacy, Hierarchy, and Technology

WRITE-EFFICIENT memories (WEM) were introduced in [2] as a model for storing and updating information on a rewritable medium. There is a cost $\varphi: \mathscr{X} \times \mathscr{X} \to \mathbb{R}_\infty$ assigned to changes of letters. A collection of subsets $\mathscr{C} = \{C_i: 1 \le i \le M\}$ of $\mathscr{X}^n$, called clouds, is an (n, M, D) WEM code, if $C_i \cap C_j = \varnothing$ for all $i \ne j$ and if

$$D_{\max} = \max_{1 \le i, j \le M} \max_{x^n \in C_i} \min_{y^n \in C_j} \sum_{t=1}^{n} \varphi(x_t, y_t) \le D. \quad (1.1)$$

$D_{\max}$ is called the maximal correction cost with respect to the given cost function. The performance of a code $\mathscr{C}$ can also be measured by two parameters, namely, the maximal cost per letter $d_{\mathscr{C}} = n^{-1} D_{\max}$ and the rate of the size $r_{\mathscr{C}} = n^{-1} \log M$. The rate achievable with a maximal per letter cost d is thus

$$R(d) = \sup_{\mathscr{C}: d_{\mathscr{C}} \le d} r_{\mathscr{C}}. \quad (1.2)$$

This is the most basic quantity (the storage capacity) of a WEM $(\mathscr{X}^n, \varphi^n)_{n=1}^{\infty}$.

For a WEM code $\mathscr{C}$, the average correction cost D_{ave} can be defined as

$$D_{\text{ave}} = \frac{1}{M^2} \sum_{1 \le i, j \le M} \frac{1}{|C_i|} \sum_{x^n \in C_i} \min_{y^n \in C_j} \sum_{t=1}^{n} \varphi(x_t, y_t) \quad (1.3)$$

Manuscript received October 29, 1992; revised July 8, 1993. This paper was presented in part at the IEEE International Workshop on Information Theory, Ithaca, NY, June 1989.

R. Ahlswede is with the Fakultät für Mathematik, Universität Bielefeld, Postfach 100131, 33501 Bielefeld, Germany.

Z. Zhang is with the Communication Sciences Institute, University of Southern California, Los Angeles, CA 90089.

IEEE Log Number 9402027.

and the average cost per letter can be defined as

$$\bar{d}_{\mathscr{C}} = n^{-1} D_{\text{ave}}. \quad (1.4)$$

The rate achievable with an average per-letter cost d is thus

$$\bar{R}(d) = \sup_{\mathscr{C}: \bar{d}_{\mathscr{C}} \le d} r_{\mathscr{C}}. \quad (1.5)$$

The main result of [2] is

$$\bar{R}(d) = R(d) = \sup_{P_{XY} \in \mathscr{P}_d} H(Y|X) \quad (1.6)$$

where $\mathscr{P}_d$ is a set of bivariate distributions

$$\mathscr{P}_d = \left\{P_{XY} \in \mathscr{P}(\mathscr{X} \times \mathscr{X}): P_X = P_Y, \mathbb{E}_\varphi(X, Y) \le d\right\}, \quad (1.7)$$

P_{XY} is the distribution of a pair of random variables (X, Y) with values in $\mathscr{X} \times \mathscr{X}$, P_X (resp., P_Y) is the distribution of X (resp., Y), $H(Y|X)$ is the conditional entropy of Y given X, and $\mathbb{E}$ denotes the expected value.

An essential ingredient of this result is a combinatorial result. We say that the hypergraph $(\Omega, \mathscr{E})$ carries M colors if there is a vertex coloring with M colors such that *all* of these colors occur in every edge. Let $M(\Omega, \mathscr{E})$ be the maximal number of colors carried by $(\Omega, \mathscr{E})$.

Coloring Lemma: The hypergraph $(\Omega, \mathscr{E})$ carries M colors if $M \le (\ln |\Omega|)^{-1} \min_{E \in \mathscr{E}} |E|$ and $M \ge 2$.

Since, in typical applications, the quantities $|\Omega|$ and $|E|$ grow exponentially in the block length n, we have $M(\Omega, \mathscr{E}) \sim \min_{E \in \mathscr{E}} |E|$. We remark that determining $M(\Omega, \mathscr{E})$ for any hypergraph $(\Omega, \mathscr{E})$ induces problems of the Ramsey type.

More generally, one can consider more general cost functions

$$\varphi^n: \mathscr{X}^n \times \mathscr{X}^n \to \mathbb{R}_\infty, \qquad n \in \mathbb{N}, \quad (1.8)$$

and, even more generally, one can combine this WEM model with the stochastic model of [12].

However, for the sake of simplicity, in this paper we stick to our original definition of a WEM. Genuine examples are the Hamming WEM, specified by $\mathscr{X} = \{0, 1\}$, and the cost function $\varphi = d_H$, the Hamming distance, and the (symmetric alternating)WUM (see [3]–[5], [9], [10], [12]) specified by

$$\varphi(x, y) = \begin{cases} 0, & \text{if } (x, y) \ne (1, 1), x, y \in \{0, 1\} \\ \infty, & \text{if } (x, y) = (1, 1). \end{cases} \quad (1.9)$$

0018-9448/94$04.00

The connection of this definition to the original definition —which comes directly from the coding problem—is clarified in the passage before Theorem K in Section IV.

Here, we follow the natural idea of letting several users operate with the same memory, that is, the space $\mathcal{X}^n$. Several constraints on the mode of these operations are considered and lead, perhaps surprisingly, to some seemingly original problems. One assumption is basic and will always be made:

The users, say $U_1, U_2, \cdots, U_s$, follow no protocol, which determines in which order they store messages. At any time instant, exactly one user has access to the memory. We address questions, which are meaningful, if the user at any time instant is any member of the prescribed set of users.

We speak of a multiuser WEM and discuss possible constraints.

Constraints on Technology: It was laser technology which led to the WUM model and thus to a specific cost function in the WEM model. It is reasonable to assume that different users have different cost functions and different thresholds for the total costs.

Common Messages: All users are supposed to write and read the same messages at any time instant.

Separate Messages Without Protection: All users always have their own messages to store. However, a user can only read what he wrote formerly, if this was not distorted by another user in the meantime. If storage is a very rare event, this still may be practical to a certain extent.

Separate Messages with Protection—Privacy: Suppose that there are two users, U_1 and U_2. At any time, where one user updates his memory with a new message, he has to guarantee that the message stored by the other user does not get distorted. In this sense, users respect each other's privacy.

Separate Messages with One-Sided Protection—Hierarchy: Here, user U_2 has to respect the privacy of user U_1, but not vice versa.

The Hierarchy Graph: It is conceivable that any two users, say U_i and U_j, do not mutually respect their privacy, that they both respect the privacy of the other, and finally, that U_i respects the privacy of U_j, but not vice versa. This can be symbolized by an undirected edge, an edge with two arrows, and a directed edge, respectively, in a graph with vertex set $\{U_1, \cdots, U_s\}$. Thus, the three foregoing cases all become special cases of this general model.

Side Information: The issue of side information has played an important role in multiuser source and channel coding. We use the notation E_+ (resp., D_+), if the encoder (resp., decoder) has side information, and the notation E_- (resp., D_-), if the encoder (resp., decoder) does not have side information. For memory cells, the side information refers to the knowledge of the contents of the memory before a new action (encoding or decoding) is taken. The results for WEM codes stated above concern the case (E_+, D_-), which seems to be the most natural. Of course, all kinds of other situations with side information can be imagined—for instance, those where the encoder knows time, that is, he knows how many updatings have been made.

Identification: We address here for the first time storage for the purpose of identification. The theory of identification via channels [18] is paralleled by a theory of identifications via memories. It should be mentioned that there are also *multitape* problems. Some are formulated in Section IX. Finally, we mention that the area of combinatorial extremal problems already has received a significant impetus from the theory of memories (cf. [6]–[8], [17]). In Section II, further questions are asked which are linked to multiuser memories.

The paper is organized as follows.

In Section II, we present a capacity formula for the WEM with several users having common messages. It is in the spirit of the coding theorem for compound channels.

Next, we present in Section III a multiuser rate region for separate messages without protection. The hard work starts in Section IV with the analysis of a WEM used by two persons, who respect each other's privacy. In particular, we derive bounds on the rate regions for cost functions satisfying the triangle inequality. We also take a closer look at the WUM. By the probabilistic method, we achieve rate pairs beyond the time-sharing bound. In another direction, we show that the sum of the rates can be made to approach the maximal possible rate $\log |\mathcal{X}|$ as the number of users increases. Originally, we conjectured this for the WUM, and there it was proved by Koschnick [11]. Serious work remains to be done. Some combinatorial problems are extracted in Section IX.

In Section V, we discuss the issue of hierarchy, and in Section VI, we focus on side information. Whereas all results indicated so far are for the case (E_+, D_-), we discuss other cases in Section VI. We present several coding theorems. Some of them in the case (E_-, D_-) are just consequences of the Diametric Theorem of [16]. Previously for the single-user WUM, this was an outstanding problem (see [9], [12]).

In section VII, we go in a new direction. We take the first steps in a theory of identification and memories. As previously done in [18] and [19], we again establish second-order coding theorems.

In Section VIII, we provide constructions of multiuser WUM codes under the complete privacy constraint. Several open problems are stated in Section IX. Finally, we include in an Appendix two old but unpublished constructions of the second author for single-user WUM codes.

II. Common Messages

User U_k $(k = 1, 2, \cdots, K)$ has his cost function $\varphi_k: \mathcal{X} \times \mathcal{X} \to \mathbb{R}_\infty$. Furthermore, he has his own cost constraint. A common $(n, M, (D_k)_{k=1}^K)$ WEM code is now a collection of subsets $\mathcal{C} = \{C_i: 1 \le i \le M\}$ of $\mathcal{X}^n$, called clouds, with $C_i \cap C_j = \emptyset$ for all $i \ne j$ and with

$$D_{k,\max} = \max_{1 \le i,j \le M} \max_{x^n \in C_i} \min_{y^n \in C_j} \sum_{t=1}^{n} \varphi_k(x_t, y_t) \le D_k \quad (2.1)$$

for $k = 1, 2, \cdots, K$.

As in Section I, $r_{\mathscr{C}} = n^{-1} \log M$ is the rate of this code and $\vec{d}_{\mathscr{C}} = n^{-1}(D_{1,\max}, \cdots, D_{K,\max})$ is the vector of maximal costs per letter. The rate achievable with a maximal per-letter cost vector $\vec{d} = (d_1, \cdots, d_K)$ is thus

$$R(\vec{d}) = \sup_{\mathscr{C}: \vec{d}_{\mathscr{C}} \le \vec{d}} r_{\mathscr{C}}. \tag{2.2}$$

As in (1.7), we now define for every k a set of bivariate distributions

$$\mathscr{P}_{d_k,k} = \left\{P_{XY} \in \mathscr{P}(\mathscr{X} \times \mathscr{X}): P_X = P_Y, \mathbb{E}_{\varphi k}(X, Y) \le d_k\right\}. \tag{2.3}$$

Furthermore, we set

$$\mathscr{P}_{\vec{d}} = \bigcap_{k=1}^{K} \mathscr{P}_{d_k,k}. \tag{2.4}$$

Here is our first result.

Theorem 1: The optimal rate for a common code is

$$R(\vec{d}) = \sup_{P_{XY} \in \mathscr{P}_{\vec{d}}} H(Y|X).$$

Proof: Replacing in [2, sect. 4–6] $S_d(x^n) = \{y^n \in \Omega: \varphi(x^n, y^n) \le nd\}$ in [2, eq. (4.1)] by

$$S_{\vec{d}}(x^n) = \{y^n \in \Omega: \varphi_k(x^n, y^n) \le nd_k \quad \text{for } k = 1, \cdots, K\} \tag{2.5}$$

where $\Omega = \bigcup_{i=1}^{M} C_i$, the proofs in conjunction with a standard argument of simultaneity also settle the present case. We skip the details because they are routine.

We have to keep in mind that we have just considered the case in which the encoder knows the previous state of the memory and the decoder does not, that is, the case (E_+, D_-).

Neither the encoder nor the decoder has any knowledge about the user. The code concept allows the users to write on the memory and to read its content in an arbitrary moving order. If, now, the encoder and the decoder know the user at each move, they can achieve as a "one-shot" rate

$$\min_k \sup_{P_{XY} \in \mathscr{P}_{d_k,k}} H(Y|X) \ge R(\vec{d}).$$

We come across the following question.

Problem 1: What is the optimal rate in this situation for any number of moves?

We also would like to see the next question answered.

Problem 2: The users want to store their own messages without protection. They cannot operate beyond $(R_1(d_1), \cdots, R_k(d_k))$ if $R_i(d_i)$ is the optimal rate for a single user U_i at threshold d_i. These optima are achieved at different letter frequencies for the words used. What now is the achievable rate region?

III. Separate Messages with Protection: Privacy

This is perhaps the most basic of our new models. Most of our results concern the case of two users. Since the extensions of our definitions to any number of users are straightforward and so are some of the results, we give the definitions now for two users in order not to be burdened with a heavy formalism. When needed, the reader will be able to add the necessary indexes. A family $\mathscr{C} = \{C_{ij}: 1 \le i \le M_1, 1 \le j \le M_2\}$ of disjoint subsets of $\mathscr{X}^n$ is an (n, M_1, M_2, d_1, d_2) *privacy code* for the users U_1 and U_2 with cost functions φ_1 and φ_2 if, for all pairs (i, j) and (i', j) [resp., (i, j')] for every $x^n \in C_{ij}$, a $y^n \in C_{i'j}$ (resp., $C_{ij'}$) exists with

$$\frac{1}{n}\varphi_1^n(x^n, y^n) \le d_1 \quad \left(\text{resp.}, \frac{1}{n}\varphi_2^n(x^n, y^n) \le d_2\right). \tag{3.1}$$

The pair (R_1, R_2) of nonnegative numbers is called an achievable pair of rates if, for every $\eta > 0$, there are privacy codes of rates $r_i = (1/n)\log M_i > R_i - \eta (i = 1, 2)$ for all large n. $\mathscr{R} = \mathscr{R}(d_1, d_2) = \mathscr{R}(d_1, d_2, \varphi_1, \varphi_2)$ is the set of all achievable pairs of rates.

Clearly, this code can be used by any one of the users to store a new message without distorting the message stored by the other user. In the sequel, we assume that

$$\varphi_1 \equiv \varphi_2 \equiv \varphi \tag{3.2}$$

and we let $M(n, d)$ stand for the maximal length of an (n, d) WEM code with cost function φ.

We formulate our first observation.

Lemma 1: When the cost function φ satisfies the triangle inequality, then for any (n, M_1, M_2, d_1, d_2) privacy code,

$$M_1 M_2 \le M(n, d_1 + d_2). \tag{3.3}$$

Thus, $\mathscr{R}(d_1, d_2) \subset \{(R_1, R_2): 0 \le R_i,\ R_1 + R_2 \le R(d_1 + d_2)\}$.

Proof: The privacy code for two users also can be viewed as a one-user code with $M_1 M_2$ messages. For any pairs (i, j) and (i', j'), we can make the transitions from (i, j) to (i', j) and then to (i', j'), for instance. Therefore, by the triangle inequality, for any $x^n \in C_{ij}$, a $y^n \in C_{i'j}$ and a $z^n \in C_{i'j'}$ can be found with

$$\varphi(x^n, z^n) \le \varphi(x^n, y^n) + \varphi(y^n, z^n). \tag{3.4}$$

The per-letter cost is at most $d_1 + d_2$.

Remark: The cost function of the symmetric WUM does not satisfy the triangle inequality. Of course, the Hamming distance does.

Now, vice versa, we can also view an $(n, M_1 \cdot M_2, d)$ one-user code as an (n, M_1, M_2, d, d) privacy code by choosing $\{1, \cdots, M_1\} \times \{1, \cdots, M_2\}$ as the index set of the clouds, We express this in terms of rates:

$$\mathscr{R}(d, d) \supset \{(R_1, R_2): 0 \le R_i, R_1 + R_2 \le R(d)\}. \tag{3.5}$$

A third simple fact is that, by space sharing, a single-user (n_1, M_1, τ_1) code $\{C_i\}$ and a single-user (n_2, M_2, τ_2) code $\{D_j\}$ can be combined to an $(n_1 + n_2, M_1, M_2, n_1\tau_1/(n_1 + n_2), n_2\tau_2/(n_1 + n_2))$ privacy code $\{C_i \times D_j\}$. We rewrite

this in terms of rates by using the substitutions $\lambda_i = n_i/(n_1+n_2)$ and $d_i = \lambda_i \tau_i$.

Lemma 2: $\mathscr{R}(d_1, d_2) \supset \{(R_1, R_2): 0 \le R_i \le \lambda_i R(d_i/\lambda_i), 0 < \lambda_i$ for $i = 1,2$ and $\sum_{i=1}^{2} \lambda_i = 1\}$.

Since $R(d)$ is increasing in d, (3.5) is implied by Lemma 2, which shows that we can do better with privacy codes than by simply changing the purpose of a single-user code. Instead of the rate pairs $(\frac{1}{2}R(d), \frac{1}{2}R(d))$, we can actually achieve the rate pair $(\frac{1}{2}R(2d), \frac{1}{2}R(2d))$. However by Lemma 1, this is even an optimal rate pair if φ satisfies the triangle inequality! Obviously, the same phenomenon can be found and stated in obvious notation for any number of users.

Theorem 2: In case K users have the same cost function φ and agree to have all the same rates and per-letter costs d, then we have for the optimal rate $R'(d)$

$$R'(d) \ge \frac{R(Kd)}{K}. \tag{3.6}$$

Moreover, if φ satisfies the triangle inequality, then equality holds here.

There is an interesting consequence for cost functions φ which take only finite values.

Corollary: For $\varphi: \mathscr{X} \times \mathscr{X} \to \mathbb{R}$ and $d > 0$

$$\lim_{K \to \infty} KR'(d) = \log |\mathscr{X}|. \tag{3.7}$$

Proof: If $Kd \ge \max_{x,y \in \mathscr{X}} |\varphi(x,y)|$, then $R(Kd) = \log |\mathscr{X}|$, and by (3.6), $KR'(d) \ge \log |\mathscr{X}|$. On the other hand, the clouds $C_{i_1 \cdots i_K}$ in a privacy code are disjoint, and therefore $\prod_{i=1}^{K} M_i \le |\mathscr{X}|^n$. In particular, we also have $KR'(d) \le \log |\mathscr{X}|$, and (3.7) is established.

Problem 3: Find the region of all achievable rates ("capacity region") $\mathscr{R}(d_1, d_2, \cdots, d_K)$. This is a formidable task already for $K = 2$ and the Hamming distance as a cost function! How good is the bound of Lemma 2?

IV. Privacy on the WUM

Since for the WUM the optimal rate is the same for any finite threshold d of the per-letter cost, Lemma 2 gives, in this case, achievability of the simple rate-sharing region

$$\mathscr{R}_S = \{(R_1, R_2): 0 \le R_i,\ R_1 + R_2 = R_{\mathrm{WUM}}\}, \tag{4.1}$$

and as an analogue to (3.6), the simple inequality

$$KR' \ge R_{\mathrm{WUM}}. \tag{4.2}$$

Theorem 3 below establishes a region bigger than $\mathscr{R}_S$. This was the basis for our conjecture that (3.7) also holds for the WUM, which has a cost function excluded in the corollary because it takes the value infinity. The conjecture was proved by Koschnick with a pretty idea [11]. We describe his construction at the end of this section because it is so brief.

Let us first notice that condition (1.9) allows us to define alternating symmetric WUM codes without any reference to φ in an appealing form.

It is a collection $\{C_i: 1 \le i \le M\}$ of disjoint subsets of $\mathscr{X}^n = \{0,1\}^n$ with the following properties.

For all i and j, for any $x^n \in C_i$, a $y^n \in C_j$ exists with

$$x^n \wedge y^n = (x_1 \wedge y_1, \cdots, x_n \wedge y_n) = (0, \cdots, 0). \tag{4.3}$$

(We remind the reader again about the passage before Theorem K in Section IV.)

From here, the definition of a privacy code (n, M, N) for the WUM reads as follows:

It is a collection $\{C_{ij}: 1 \le i \le M, 1 \le j \le N\}$ of disjoint subsets of $\mathscr{X}^n$, called clouds, with the properties that for all (i,j) and (i',j) [resp., (i,j')], for every $x^n \in C_{ij}$, a $y^n \in C_{i'j}$ (resp., $C_{ij'}$) exists so that (4.3) holds. (4.4)

We denote the set of achievable pairs of rates for these codes by $\mathscr{R}^2_{\mathrm{WUM}}$.

Throughout this paper, we use the "sequence" and "subset" notation interchangeably. In "subset" notation, the C_i's are disjoint families of subsets of $\{1,2,\cdots,n\}$.

Theorem 3: $\mathscr{R}^2_{\mathrm{WUM}} \supset \{(R_1, R_2): 0 \le R_i \le \frac{1}{2}$ for $i = 1,2;$ $R_1 + R_2 \le h(\frac{1}{4}) = 0.813\cdots\}$.

Remark: Since $R_{\mathrm{WUM}} = 0.694\cdots$, the new region exceeds $\mathscr{R}_S$ not everywhere.

Of course, the convex hull of the union of both regions is again achievable.

Proof: It may be helpful for grasping the idea of the following proof to first take a look at the code construction in Section VIII. We describe our random selection of the clouds. They will have *two elements*. It suffices to consider even n. Set $n = 2k$ and $\mathscr{N} = \{1,2,\cdots,n\}$. Choose independently according to the uniform distribution on $\binom{\mathscr{N}}{k}$ $M + N$ sets. Call the first M sets $S_1, \cdots, S_M$ and the last N sets $T_1, \cdots, T_N$. Define, now, for any set $A \subset \mathscr{N}$,

$$A^1 = A \quad \text{and} \quad A^0 = A^c \tag{4.5}$$

where "c" denotes complementation in $\mathscr{N}$. With this convention, we introduce the sets

$$D_{ij}^{\alpha\beta} = S_i^{\alpha} \cap T_j^{\beta} \qquad \text{for } \alpha, \beta \in \{0,1\}. \tag{4.6}$$

Clearly, $|D_{ij}^{11}| = |D_{ij}^{00}|$, $|D_{ij}^{01}| = |D_{ij}^{10}|$.

If, now, $|D_{ij}^{11}| \ge \frac{1}{4}n$, then define

$$D_{ij}^{(1)} = D_{ij}^{11} \quad \text{and} \quad D_{ij}^{(2)} = D_{ij}^{00}. \tag{4.7}$$

Otherwise, we have $|D_{ij}^{10}| \ge \frac{1}{4}n$, and we define

$$D_{ij}^{(1)} = D_{ij}^{10} \quad \text{and} \quad D_{ij}^{(2)} = D_{ij}^{01}. \tag{4.8}$$

For $C \subset \mathscr{N}$, $\frac{1}{2}n \ge |C| \ge \frac{1}{4}n$, define

$$L(C) = \left\{(i,j) \in [1,\cdots,M] \times \{1,\cdots,N\}: D_{ij}^{(1)} = C \text{ or } D_{ij}^{(2)} = C\right\}. \tag{4.9}$$

Clearly, by this definition, for all $(i,j) \in \{1,\cdots,M\} \times \{1,\cdots,N\}$,

$$(i,j) \in L\left(D_{ij}^{(1)}\right) \cap L\left(D_{ij}^{(2)}\right). \tag{4.10}$$

If, now,

$$L\left(D_{ij}^{(1)}\right) = L\left(D_{ij}^{(2)}\right) = \{(i,j)\},$$

then define

$$C_{ij} = \left\{D_{ij}^{(1)}, D_{ij}^{(2)}\right\}. \tag{4.11}$$

Let us pause a moment and realize that, by our definitions, in case (4.11) holds for *all* $(i,j) \in \{1,\cdots,M\} \times \{1,\cdots,N\}$, then these C_{ij}'s define a privacy WUM code as introduced in (4.4). However, this need not be the case or, in other words, for some C, we may have $|L(C)| > 1$. For some C, called *regular*, we can remove this ambiguity, and for other C, called *irregular*, we cannot. If irregular C are there, then the chosen collection $\{S_1,\cdots,S_M;T_1,\cdots,T_N\}$ is just bad.

We now describe the regular C's. For them, we can remove ambiguity by using suitable neighbors. Define

$$\mathcal{L}(C) = \{C' : |C\,\Delta C'| = 1, C' \subset C, \nexists\, C'' \neq C \text{ with } |C''\,\Delta C'| \in \{0,1\}, C'' \supset C' \text{ and } L(C'') \neq \emptyset\}. \tag{4.12}$$

If, now, $|L(C)| \leq |\mathcal{L}(C) \cup \{C\}| = \mathcal{L}(C)| + 1$, then choose any injective map $\Psi_C : L(C) \to \mathcal{L}(C) \cup \{C\}$. Notice that the members of $\mathcal{L}(C)$ have the following properties:

(a) they are contained in C, but are different from C by one element exactly,

(b) the do not equal any $D_{ij}^{(1)}$ or $D_{ij}^{(2)}$,

(c) the supersets different from C, which differ by exactly one element from it, also do not equal any $D_{ij}^{(1)}$ or $D_{ij}^{(2)}$.

Since C occurs $|L(C)|$ times, we can resolve this conflict by using it once and replacing it otherwise by the members of $\mathcal{L}(C)$. If both $D_{ij}^{(1)}$ and $D_{ij}^{(2)}$ are regular, then we can therefore define

$$C_{ij} = \left\{\Psi_{D_{ij}^{(1)}}(i,j), \Psi_{D_{ij}^{(2)}}(i,j)\right\}. \tag{4.13}$$

The privacy WUM code is thus well defined if there are no irregular C's. We now estimate Prob (there are no irregular $C \subset \mathcal{N}$) from below. A key role in this analysis is played by the condition

$$\max\left(M2^{-\frac{1}{2}n}, N2^{-\frac{1}{2}n}, MN2^{-2n}\binom{n-|C|}{\frac{1}{2}n-|C|}\binom{\frac{1}{2}n}{|C|}\right) < 2^{-\epsilon n}. \tag{$*$}$$

Claim 1: Prob $(|L(C)| \geq \epsilon n) \leq 2^{-\delta n(3/2)}$ for some constant $\delta > 0$ if $(*)$ holds. We first verify this.

Let us write $L(C) = \{(i_1,j_1),\cdots,(i_l,j_l)\}$, and let us consider the bipartite graph $(\{1,2,\cdots,M\},\{1,2,\cdots,N\},L(C))$. Recall König's Theorem, which says that the maximal number η of independent edges in a bipartite graph equals the minimum number $\mu + \nu$ of points covering all edges, that is,

$$\eta = \mu + \nu. \tag{4.14}$$

The total number of edges is l. If, now, $\eta < \sqrt{l}$, then by (4.14),

$$\mu + \nu < \sqrt{l} \quad \text{or} \quad \frac{l}{\mu+\nu} \geq \sqrt{l}.$$

Hence, either there is a vertex in $\{1,2,\cdots,M\}$ covering at least $\sqrt{l}$ edges, or there are $\sqrt{l}$ independent edges, or there is a vertex in $\{1,\cdots,N\}$ covering at least $\sqrt{l}$ edges.

If, now, $l \geq \epsilon n$, then choose

$$s = \lceil \sqrt{\epsilon n} \rceil. \tag{4.15}$$

Consequently, either we have event E_1: for some i and $j^{(1)},\cdots,j^{(s)}$

$$\{(i,j^{(t)}) : 1 \leq t \leq s\} \subset L(C)$$

or we have event E_2: there are sets of indexes $I = \{i^{(1)},\cdots,i^{(s)}\}$, $J = \{j^{(1)},\cdots,j^{(s)}\}$ with $\{(i^{(t)},j^{(t)}) : 1 \leq t \leq s\} \subset L(C)$, or we have event E_3: for some j and $i^{(1)},\cdots,i^{(s)}$

$$\{(i^{(t)},j) : 1 \leq t \leq s\} \subset L(C).$$

Therefore, we have

$$\text{Prob}\,(|L(C)| \geq \epsilon n) \leq \sum_{i=1}^{3} \text{Prob}\,(E_i). \tag{4.16}$$

One readily calculates that

$$\text{Prob}\,(E_1) \leq \binom{M}{1}\binom{N}{s}\left(2^{-n+0(\log n)}\binom{\frac{1}{2}n}{|C|}\right)^s,$$

$$\text{Prob}\,(E_3) \leq \binom{N}{1}\binom{M}{s}\left(2^{-n+0(\log n)}\binom{\frac{1}{2}n}{|C|}\right)^s,$$

$$\text{Prob}\,(E_2) \leq \binom{MN}{s}\left(2^{-2n+0(\log n)}\binom{n-|C|}{\frac{1}{2}n-|C|}\binom{\frac{1}{2}n}{|C|}\right)^s.$$

This, together with $(*)$, implies

$$\text{Prob}\,(|L(C)| \geq \epsilon n) \leq 3 \cdot 2^{-\epsilon n s + s\cdot 0(\log n)} \leq 2^{-\delta n^{\frac{1}{2}}}.$$

Claim 2: Prob $(|\mathcal{L}(C)| \leq \epsilon n) \leq 2^{-\delta' n(3/2)}$ for some constant $\delta' > 0$ if $(*)$ holds.

If $|\mathcal{L}(C)| \leq \epsilon n$, then there are at least $\frac{1}{4}n - \epsilon n > \frac{1}{5}n$ C^* with $|C^*\,\Delta C| \leq 2$ and $L(C^*) \neq \emptyset$. Choose, now, $s = \lceil \sqrt{n/5} \rceil$.

Considering $U(C) = \{C^* : |C^*\,\Delta C| \leq 2, |L(C^*)| \geq 1\}$, we can distinguish again three events.

Event F_1: For some i and $j^{(1)},\cdots,j^{(s)}$

$$(i,j^{(t)}) \in L(C^{(t)}), \quad C^{(t)} \in (C) \qquad \text{for } 1 \leq t \leq s.$$

Event F_2: For some j and $i^{(1)},\cdots,i^{(s)}$

$$(i^{(t)}), j^{(1)} \in L(C^{(t)}), \quad C^{(t)} \in U(C) \qquad \text{for } 1 \leq t \leq s.$$

Event F_3: There are sets of indexes $I = \{i^{(1)},\cdots,i^{(s)}\}$, $J = \{j^{(1)},\cdots,j^{(s)}\}$ such that

$$(i^{(t)},j^{(t)}) \in L(C^{(t)}), \quad C^{(t)} \in U(C) \qquad \text{for } 1 \leq t \leq s.$$

We have, therefore,

$$\text{Prob}(|\mathscr{L}(C)| \le \epsilon n) \le \sum_{i=1}^{3} \text{Prob}(F_i). \quad (4.17)$$

One calculates that, under (*),

$$\text{Prob}(F_1) \le \binom{0(n^2)}{\sqrt{\frac{n}{5}}}\binom{M}{1}\binom{N}{\sqrt{\frac{n}{5}}} \cdot \left(2^{-n+0(\log n)} \cdot \binom{\frac{1}{2}n}{|C| \pm 2}\right)^{\sqrt{n/5}} \le 2^{-\delta' n(3/2)}.$$

Similarly, $\text{Prob}(F_2) \le 2^{-\delta' n(3/2)}$, and finally,

$$\text{Prob}(F_3) \le \binom{0(n^2)}{\sqrt{\frac{n}{5}}}\binom{MN}{\sqrt{\frac{n}{5}}}\left(2^{-2n+0(\log n)} \cdot \binom{n-|C| \pm 2}{\frac{1}{2}n \pm 2 - |C|} \cdot \binom{\frac{1}{2}n}{|C| \pm 1}\right)^{\sqrt{n/5}} \le 2^{-\delta' n(3/2)}$$

and thus Claim 2.

The two claims imply $\mathbb{E}|\{C: |L(C) \ge \epsilon n\}| + \mathbb{E}|\{C: |\mathscr{L}(C)| \le \epsilon n\}| \le 2^n \cdot 2^{-\delta n(3/2)} + 2^n \cdot 2^{-\delta n(3/2)}$, and therefore the expected values tend to 0 as n tends to infinity. In particular, it becomes smaller than 1, and thus for large n with positive probability for all C $|\mathscr{L}(C)| > \epsilon n > |L(C)|$ and all C must be regular. Hence, a privacy code exists if (*) holds. Now, for (R_1, R_2) with $R_i \le \frac{1}{2} - \epsilon$ and $R_1 + R_2 \le 2 - \epsilon - (1/n) \log \max_{|C| \ge (1/4)n} \binom{n-|C|}{\frac{1}{2}n - |C|}\binom{\frac{1}{2}n}{|C|}$, (*) is valid.

Observe next that

$$\max_{|C| \ge \frac{1}{4}n} \binom{n-|C|}{\frac{1}{2}n|C|}\binom{\frac{1}{2}n}{|C|} = \binom{\frac{3}{4}n}{\frac{1}{4}n}\binom{\frac{1}{2}n}{\frac{1}{4}n}$$

and that $\lim_{n\to\infty} (1/n) \log \binom{\frac{3}{4}n}{\frac{1}{4}n}\binom{\frac{1}{2}n}{\frac{1}{4}n} = 2 - h(\frac{1}{4})$. The proof is complete.

Originally, WUM codes dealt with a situation arising in laser technology, where during one updating, only 0's or only 1's can be printed into the cells of the memory. In particular, this has led to the concept of an *alternating WUM code*:

A family $\mathscr{C} = \{C_1, \cdots, C_M\}$ of disjoint subsets of $\{0,1\}^n$ is an alternating WUM code if

(i) $C_i = T_{i0} \cup T_{i1}$ for $1 \le i \le M$,

(ii) for all (i,j) and any $x^n \in T_{i0}$ (resp., T_{i1}) there is a $y^n \in T_{j1}$ (resp., T_{j0}) with $y^n \ge x^n$ (resp., $y^n \le x^n$).

An alternating WUM code is called *symmetric* if, for $i = 1, \cdots, M$,

$$T_{i1} = \bar{T}_{i0} = \{\bar{x}^n: x^n \in T_{i0}\}.$$

Here, $\bar{x}^n$ is obtained from x^n by exchanging 0's and 1's.

Obviously, a symmetric code is specified solely by the collection of subsets $\{T_{i0}\}$. T_{i0}'s are used when we write 1's and T_{i1}'s are used when we write 0's. We can always use one additional bit of information to indicate which letter we are writing. In this sense, it does not matter whether T_{i0} and T_{j1} intersect or not. We need only the disjointness among T_{i0}'s and the disjointness among T_{i1}'s. Now, for $x^n \in T_{i0}$ and $y^n \in \bar{T}_{j0}$ with $x^n \le y^n$, we have $\bar{y}^n \in T_{j0}$ and $x^n \wedge \bar{y}^n = (0,0,\cdots,0)$. Therefore, we can use the *alternative* definition for an alternating symmetric WUM code given in (1.9) or (4.3). Since it is often easier to handle, we use in this paper the definition (1.9), bearing in mind that we can always easily construct a code in the sense of the former definition from a code in our new sense.

If $C_i \cap \bar{C}_j = \emptyset$ for all i and j, which is the case for the codes of Willems, Vinck, and Simonyi, we do not even need the additional bit of information.

We now present the positive answer to our conjecture that (3.7) also holds for WUM.

Theorem K [11]: We can achieve with a K user privacy WUM code the rate vector $(\frac{1}{K+1}, \cdots, \frac{1}{K+1})$, and thus total rate $\frac{1}{K+1}$.

Proof: We describe in the language of our codes Koschnick's construction [11] of an $(n, M_1, \cdots, M_K)$ code with

$$n = (K+1)s + 2 \cdot \lceil \log_2 (K+1)! \rceil \quad (4.18)$$

and

$$M_1 = 2^s \qquad \text{for } i = 1,2,\cdots,K. \quad (4.19)$$

Divide the memory of size n into $K+1$ parts $A_1, \cdots, A_{K+1}$, each of size s, and one part B of size $2 \cdot \lceil \log_2 (K+1)! \rceil$. At any time, the messages of the K users are represented by K of the $K+1$ parts A_i of the memory. The remaining A block contains no information; it has only cells with 0 entries. In the B block, with a single-user WUM it is stored, which A block is free and which A block contains the message of which user (note that $2\lceil \log_2 (K+1)! \rceil$ bits are sufficient for this).

Updatings are performed as follows. If user U_i wants to update his message stored by the memory, he first reads the content of block B and finds which A block contains his currently stored message—say, this is block A_r—and which one is free. After storing his new s bits in the free block and printing 0's only in the block A_r, he stores in block B again which A block relates to which user. The updating is complete.

Finally, by (4.18) and (4.19) for fixed K,

$$\lim_{n\to\infty} \frac{1}{n} \log M_i = \frac{1}{K+1}.$$

V. A Hierarchy Code for the WEM

We now come to two users, U_1 and U_2, who both store messages in the memory, but only U_1 enjoys protection of his messages by U_2. To simplify matters, we assume that both users have the same cost function φ.

An (n, M_1, M_2, d_1, d_2) hierarchy code is a collection $\{C_{ij}: 1 \le i \le M_1, 1 \le j \le M_2\}$ of disjoint subsets of $\mathscr{X}^n$ with the following properties:

(a) the collection $\{C_i: 1 \le i \le M_1\}$, where $C_i = \bigcup_{j=1}^{M_2} C_{ij}$, is an (n, M_2, d_1) WEM code for the single-user U_1;

(b) for every i, $1 \le i \le M_1$, the collection $\{C_{ij}: 1 \le j \le M_2\}$ is an (n, M_2, d_2) WEM code for the user U_2.

At any time instant, any one of the users can operate on the memory. User U_1 updates his messages via his code. The message stored by U_2 is of no concern for him. On the other hand, user U_2 has to protect the message, say i, of user 1. This means he can only make changes within C_i, where he stores his new message by the rules of the *local* code $\{C_{ij}: 1 \le j \le M_2\}$. Let us denote the rate region by $\mathscr{R}^*(d_1, d_2)$. Obviously, $\mathscr{R}^*(d_1, d_2) \supset \mathscr{R}(d_1, d_2)$, and we derive the following from Lemma 2.

Lemma 2:* If φ is not degenerate, that is, $\varphi(x, x) = 0$ for $x \in \mathscr{X}$, $\mathscr{R}^*(d_1, d_2) \supset \{(R_1, R_2): 0 \le R_1 \le \lambda_i R(d_i/\lambda_i)$, $0 < \lambda_i$ for $i = 1, 2$ and $\sum_{i=1}^2 \lambda^1 = 1\}$.

However, perhaps surprisingly, the upper bound of Lemma 1 also extends.

Lemma 1:* When the cost function φ satisfies the triangle inequality, then for any (n, M_1, M_2, d_1, d_2) hierarchy code

$$M_1 M_2 \le M(n, d_1 + d_2).$$

Thus, $\mathscr{R}^*(d_1, d_2) \subset \{(R_1, R_2): 0 \le R_i, R_1 \le R(d_1 + d_2)\}$.

Proof: The hierarchy code also can be viewed as a one-user code with $M_1 M_2$ messages. The verification differs slightly from the one for the privacy code. For any pairs (i, j) and (i', j'), we can make a transition from $C_{ij} \subset C_i$ to $C_{i'}$ and thus to $C_{i'j''}$ for some j'' (possibly different from j). But now, we still can make the transition via the local code to $C_{i'j'}$.

The argument can be applied to any number of users with a *linear hierarchy structure*, that is, messages of users with a lower number are to be protected by users with higher numbers.

Theorem 2:* In case K users have a linear hierarchy structure and the same cost function satisfying the triangle inequality, then the optimal common rate for per-letter cost d equals $(1/K)R(Kd)$.

VI. No Side Information at the Encoder and the Decoder, But the Encoder Can Use Space Bars

We consider now the case (E_-, D_-) described in the Introduction. All users have the same cost function φ. We denote by $R_-(d)$ [resp., $\bar{R}_-(d)$] the optimal rate for a single user and threshold d, in case the maximal (resp., average) costs are considered. Here, $C = \{c_i: 1 \le i \le M\}$ with $c_i \in \mathscr{X}^n$ is an $(n, M, \bar{d})$ WEM code if

$$D_{\text{ave}}(C) = \frac{1}{M^2} \sum_{i=1}^{M} \sum_{j=1}^{M} \varphi(c_i, c_j) \le n\bar{d}, \qquad (6.1)$$

and it is an (n, M, d) code if

$$\varphi(c_i, c_j) \le nd \quad \text{for } i, j = 1, 2, \cdots, M. \qquad (6.2)$$

In recent work [16] and as a result of an entirely different direction of research, $\bar{R}_-(d)$ was characterized for all cost functions $\varphi: \mathscr{X} \times \mathscr{X} \to \mathbb{R}$ as follows.

Consider a constant ν, $0 \le \nu \le 1$ and two probability distributions P and P' on $\mathscr{X}$. $(x_1, x_2, \cdots, x_n) \in \mathscr{X}^n$ is said to be of the mixed type $(\nu P, (1 - \nu)P')$ if $(x_1, \cdots, x_{\lfloor \nu n \rfloor})$ is of type P and $(x_{\lfloor \nu n \rfloor + 1}, \cdots, x_n)$ is of type P' (that is, has relative frequencies specified by P'). The sets

$$T_n(\nu, P, P') = \{x^n \in \mathscr{X}^n: x^n \text{ is of mixed type } (\nu P, (1 - \nu)P')\}$$

have a rate

$$R(\nu, P, P') = \nu H(P) + (1 - \nu)H(P')$$

and an average cost

$$D_{\text{ave}}\left(T_n(\nu, P, P') = n\left(\nu \sum_{x, u \in \mathscr{X}} P(x)P(y)\varphi(x, y) + (1 - \nu) \sum_{x, y \in \mathscr{X}} P'(x)P'(y)\varphi(x, y)\right) + o(n).\right.$$

Theorem AA: $\bar{R}_-(\bar{d}) = \max\{R(\nu, P, P'): (\nu, P, P')$ with $\sum_{x, y \in \mathscr{X}}(P(x)P(y) + (1 - \nu)P'(x)P'(y) \cdot \varphi(x, y) \le \bar{d}\}$.

Remarks: We stated in [2, eq. (9.1)] a simpler formula for $\bar{R}(d)$. It holds for special cost functions such as the Hamming distance in the binary case, but not in general. $R_-(d)$ is known in some metric cases [7], for instance in the binary Hamming case.

Recently, a solution of the diametric problem in the average has also been found for several distance and cross-distance constraints [20], that is, a multiuser model.

Inspection of Lemmas 1, 2 and Lemmas 1*, 2* shows that they can be extended much further. One observation is that, for them to hold, no *formula for the underlying single user rate function is needed*, and another observation is that *space sharing must be possible*. In case E_+, this is obviously always possible because the encoder writes in one part, say B_1, of the memory, and leaves the imprints in the other part, say B_2, invariant. He can do the latter at no cost if φ is not degenerate. In case E_-, however, he does not know the imprints, especially not in B_2. Therefore, he does not know what to write in order to leave them invariant. *If we allow the encoder to use space bars, then this simply means that we allow him to print nothing in certain cells such that their content, unknown to him, does not change.* We symbolize this option by $E_\square$. Clearly, in this case, space sharing is possible. The single-user rate functions are denoted by $R_\square(d)$ and $\bar{R}_\square(d)$.

In case E_-, there is no way in which the users keep their privacy. The hierarchy constraint can be met if the "slave" is in case E_+. (The boss cannot read, but the slave

has to be able to read in order to respect the wishes of the boss.) This leads to a funny code concept.

We concentrate now on the side information $(E_\square, D_-)$. In case of privacy, we denote the rate regions by $\mathscr{R}_\square(d_1, d_2)$ and $\overline{\mathscr{R}}_\square(d_1, d_2)$. We add a star if we have hierarchy. It saves notation if we introduce the region

$$\mathscr{T}(R) = \{(R_1, R_2): 0 \le R_i, R_1 + R_2 \le R\}. \quad (6.3)$$

Lemma 3: If φ satisfies the triangle inequality, then
(a) $\mathscr{R}_\square(d_1, d_2) \subset \mathscr{T}(R_\square(d_1 + d_2))$
(b) $\overline{\mathscr{R}}_\square(d_1, d_2) \subset \mathscr{T}(\overline{R}_\square(d_1 + d_2))$
(c) $\mathscr{R}^*_\square(d_1, d_2) \subset \mathscr{T}(R_\square(d_1 + d_2))$
(d) $\overline{\mathscr{R}}^*_\square(d_1, d_2) \subset \mathscr{T}(\overline{R}_\square(d_1 + d_2))$.

Proof: Since $\mathscr{R}_\square(d_1, d_2) \subset \mathscr{R}^*_\square(d_1, d_2)$ and $\overline{\mathscr{R}}_\square(d_1, d_2) \subset \overline{\mathscr{R}}^*_\square(d_1, d_2)$, it suffices to establish the last two inclusions.

(c) From the point of view of the decoder, there is a collection $\{C_{ij}: 1 \le i \le M_1, 1 \le j \le M_2\}$ of disjoint subsets of $\mathscr{X}^n$. Elements of C_{ij} store message i for U_1 and message j for U_2. The elements of $C_i = \bigcup_{j=1}^{M_2} C_{ij}$ store message i for U_1. If the code has parameters (n, M_1, M_2, d_1, d_2), then we can build a single-user code with parameters $(n, M_1 \cdot M_2, d_1 + d_2)$. To see this, let us suppose that c_{ij} is the imprint not known to the users. We want to store (i', j'). First, let U_1 store i' according to the rules of the code. This results in some imprint $c_{i'j''}$. Now, let U_2 store j'. This results in some imprint $c_{i'j'}$. Furthermore,

$$\varphi(c_{ij}, c_{i'j'}) \le \varphi(c_{ij}, c_{i'j''}) + \varphi(c_{i'j''}, c_{i'j'}) \le nd_1 + nd_2. \quad (6.4)$$

(d) If the average per-letter costs are d_1 and d_2, then

$$\frac{1}{(M_1M_2)^2} \sum_{i=1}^{M_1} \sum_{j=1}^{M_2} \sum_{i'=1}^{M_1} \sum_{j'=1}^{M_2} \varphi(c_{ij}, c_{i'j'}) \le nd_1 + nd_2.$$

Let E_o be any side information induding $E_\square$, that is, the side information which makes space sharing possible, and let us indicate this information with a circle in the notations for regions.

Lemma 4: If φ is not degenerate, then

$$\mathscr{R}_o(d_1, d_2) \supset \left\{(R_1, R_2): 0 \le R_i \le \lambda_i R_o\left(\frac{d_i}{\lambda_i}\right), 0 < \lambda_i \le 1, \Sigma\lambda_i = 1\right\},$$

$$\mathscr{R}^*_o(d_1, d_2) \supset \left\{(R_1, R_2): 0 \le R_i \le \lambda_i, R_o\left(\frac{d_i}{\lambda_i}\right), 0 < \lambda_i \le 1, \Sigma\lambda_i = 1\right\}.$$

The same relations hold for average costs.

Proof: As usual, by time sharing.

It is now clear how to produce from these two lemmas results like Theorems 2, 2*. We address one striking case here.

Theorem 4: For K users with complete privacy constraints and a cost function, which is a metric, we have in case $(E_\square, D_-)$ as the optimal common rate for per-letter cost d

$$\frac{1}{K} R_\square(Kd)\left(\lim_{K\to\infty} R_\square(Kd) = \log|\mathscr{X}|\right).$$

Problem 4: Consider coding problems for common messages (see Section II) in case (E_-, D_-) and average costs constraint.

Problem 5: How does $R_\square(d)$ relate to $\overline{R}_\square(d)$? Are there φ for which these quantities are different?

Problem 6: Suppose in case (E_-, D_-) the user is informed whether an intended writing is possible, given the cost constraint and the imprint (unknown to him). Are there meaningful results?

VII. Identification on the WEM

We assume here familiarity with the notions and results of [18].

The memory is now not used for the storage of messages, but for the identification of any one of M objects.

Now, just observe that in the case of the maximal per-letter cost criterion, all storage problems (single- and multiuser, privacy, hierarchy, common messages, various kinds of side information) can all be viewed as error-free transmission problems over a noiseless channel with senders $U_1, \cdots, U_K$ and the decoder as receiver.

Let us assume that the respective codes are specified. To fix ideas, let us address the single-user case now. Let its message set be $\mathscr{M} = \{1, \cdots, M\}$. Then there are $N = 2^{h(\epsilon)M}$ subsets $\{P_j: 1 \le j \le N\}$ of cardinality $M/2$ with symmetric difference of cardinality at least ϵM. Let $\mathscr{D} = \{(D_j, Q_j): 1 \le j \le N\}$, where Q_j is the uniform distribution on D_j, be the random encodings for the objects $1, 2, \cdots, N$. We know from [18] that this gives a "good" randomized identification code for the noiseless channel with second-order rate $1/n \log\log 2^{h\epsilon M} \sim 1/n \log M = R(d) + o(n)$. We also know by the converse result of [18] that this is the best possible. With every updating, these randomized encodings are employed.

The same can be done with several users in any case E_o. Thus, the regions $\mathscr{R}_o(d_1, d_2)$ are achievable as regions for second-order rate pairs. Also, Lemma 3 (a), (b) and Lemma 4 extend to second-order regions. We summarize this.

Theorem 5: If φ is a metric, then the second-order identification regions satisfy

$$\left\{(R_1, R_2): o \le R_i \le \lambda_i R_\square\left(\frac{d_i}{\lambda_i}\right), o < \lambda_i \le 1, \Sigma\lambda_i = 1\right\}$$

$$\subset \mathscr{R}^2_\square(d_1, d_2) \subset \mathscr{R}^{*2}_\square(d_1, d_2) \subset \mathscr{T}(\mathscr{R}_\square(d_1 + d_2)).$$

In particular, for $\lambda_i = \frac{1}{2}$, $d_1 = d_2 = d(\frac{1}{2}R_\square(2d), \frac{1}{2}R_\square(2d))$ is an optimal identification pair.

VIII. Constructions of Multiuser WUM Codes Under Privacy Constraints

We now consider symmetric alternating WUM codes as defined in Section IV. For the history of this concept, the reader is also advised to consult the Appendix. Since throughout this section *all* users keep their privacy, we simply speak of WUM codes.

We begin with (n, M, N), that is, two user WUM codes of blocklength n and message sets of sizes M and N.

We use both the subset and the sequence notation. It may be helpful to start with a simple example.

(6, 3, 4) Two-User WUM Code: The entries in the following table are the sets C_{ij} $(1 \le i \le 4, 1 \le j \le 3)$.

$j \backslash i$	1	2	3	4
1	{1,2,3}	{1,2}	{1,3}	{2,3}
	{4,5,6}	{4,5}	{4,6}	{5,6}
2	{3}	{1,2,6}	{3,5}	{1,6}
	{6}	{2,4,5}	{2,6}	{3,4}
3	{5}	{1}	{1,3,5}	{1,5}
	{2}	{4}	{2,4,6}	{2,4}

The total rate is $\frac{1}{6}\log 3 \cdot 4 = 0{,}5975\cdots$.

The idea used to construct this code is also useful for the construction of the two two-user codes below, as well as for the proof of a random coding theorem for two-user WUM in Section IV. This basic idea can be described for the (6,3,4) code as follows. Suppose that the first user has four messages. For each message of the first user, we choose a subset of $\{1,\cdots,6\}$ and denote it by X_i $(1 \le i \le 4)$. For each message of the second user, we also choose a subset of $\{1,\cdots,6\}$ and denote it by Y_i $(1 \le i \le 3)$. We call these two collections of subsets the basis of the code. Then we define either $C_{ij} = \{X_i \cap Y_j, X_i^c \cap Y_j^c\}$ or $C_{ij} = \{X_i \cap Y_j^c, X_i^c \cap Y_j\}$. Obviously, if all of the sets C_{ij} so defined are disjoint, then $\{C_{ij}: 1 \le i \le 4, 1 \le j \le 3\}$ forms a two-user WUM code. For our (6,3,4) code, we use $X_1 = \{1,2,3\}$, $X_2 = \{1,2,6\}$, $X_3 = \{1,3,5\}$, $X_4 = \{2,3,4\}$ and $Y_1 = \{1,2,3\}$, $Y_2 = \{1,2,6\}$, $Y_3 = \{1,3,5\}$. When we construct the code, all we need to take care of is the right choice for C_{ij} between the two possible methods for each pair (i, j).

The construction of the next two codes is quite similar, even with respect to the choices of the X_i's and the Y_i's.

(8, 6, 6) Two-user WUM Code: We take

$$\begin{aligned} X_1 &= \{1,2,3,4\}, \quad \text{and} \quad Y_1 = \{1,2,3,4\},\\ X_2 &= \{1,2,3,8\}, \qquad\quad\ Y_2 = \{1,2,3,8\},\\ X_3 &= \{1,2,4,7\}, \qquad\quad\ Y_3 = \{1,2,4,7\},\\ X_4 &= \{1,3,4,6\}, \qquad\quad\ Y_4 = \{1,2,7,8\},\\ X_5 &= \{2,3,4,5\}, \qquad\quad\ Y_5 = \{1,3,6,8\},\\ X_6 &= \{2,5,7,8\}, \qquad\quad\ Y_6 = \{1,4,6,7\}, \end{aligned}$$

Define either

$$(*) \quad C_{ij} = \{X_i \cap Y_j, X_i^c \cap Y_j^c\}$$

or

$$(**) \quad C_{ij} = \{X_i \cap Y_j^c, X_i^c \cap Y_j\}$$

except for $(i, j) = (6, 2)$, where we set $C_{62} = \{\varnothing\}$. The code is defined through the following table. The entries of the table are either $*$ or $**$, indicating which formula is used to form the set C_{ij}, except for C_{62}, where the entry is the set $\{\varnothing\}$.

$j \backslash i$	1	2	3	4	5	6
1	*	*	*	*	*	*
2	**	*	*	*	**	{∅}
3	**	**	*	*	**	*
4	**	*	*	**	**	*
5	**	*	**	*	**	*
6	**	**	*	*	**	*

The total rate is $\frac{1}{8}\log 6 \cdot 6 = 0{,}6463\cdots$.

(10, 6, 16) Two-User WUM Code: The construction of this code is similar to the first two two-user codes. To choose the basis, we divide the ten positions into two equal parts, $\{1, 2, 3, 4, 5\}$ and $\{6, 7, 8, 9, 10\}$. For a subset of the first part, say $Z = \{1, 2, 5\}$, we denote $\{3, 4\}$ by Z^c and $\{8, 9\}$ by $5 + Z^c$, and we define $\bar{Z} = \{1, 2, 5, 8, 9\} = Z \cup (5 + Z^c)$. For this code, we take as X_i's the six $\bar{Z}$'s such that the cardinalities of the corresponding Z's are greater than or equal to 4, and as Y_j's the 16 $\bar{Z}$'s such that the cardinalities of the corresponding Z's are greater than or equal to 3.

$$\begin{aligned} X_1 &= \{1,2,3,4,5\}, & Y_1 &= \{1,2,3,4,5\}, & Y_9 &= \{1,2,5,8,9\},\\ X_2 &= \{1,2,3,4,10\}, & Y_2 &= \{1,2,3,4,10\}, & Y_{10} &= \{1,3,4,7,10\},\\ X_3 &= \{1,2,4,5,9\}, & Y_3 &= \{1,2,3,5,9\}, & Y_{11} &= \{1,3,5,7,9\},\\ X_4 &= \{1,2,4,5,8\}, & Y_4 &= \{1,2,4,5,8\}, & Y_{12} &= \{1,4,5,7,8\},\\ X_5 &= \{1,3,4,5,7\}, & Y_5 &= \{1,3,4,5,7\}, & Y_{13} &= \{2,3,4,6,10\},\\ X_6 &= \{2,3,4,5,6\}, & Y_6 &= \{2,3,4,5,6\}, & Y_{14} &= \{2,3,5,6,9\},\\ & & Y_7 &= \{1,2,3,9,10\}, & Y_{15} &= \{2,4,5,6,8\},\\ & & Y_8 &= \{1,2,4,8,10\}, & Y_{16} &= \{3,4,5,6,7\}. \end{aligned}$$

The code is given in the following table by showing which formula is used to form the sets C_{ij}.

$j \backslash i$	1	2	3	4	5	6
1	*	* *	* *	* *	* *	* *
2	*	*	* *	* *	* *	* *
3	*	*	*	* *	* *	* *
4	*	*	*	*	* *	* *
5	*	*	*	*	*	* *
6	*	*	*	*	*	*
7	* *	*	*	* *	* *	* *
8	* *	*	* *	*	* *	* *
9	* *	* *	*	*	* *	* *
10	* *	*	* *	* *	*	* *
11	* *	* *	*	* *	*	* *
12	* *	* *	* *	*	*	* *
13	* *	*	* *	* *	* *	*
14	* *	* *	*	* *	* *	*
15	* *	* *	* *	*	* *	*
16	* *	* *	* *	* *	*	*

For this code, the sum of the two rates is $0.6585\cdots$. This is the best two-user WUM code we know.

For more than two users, it is convenient to write symmetric alternating WUM codes in the following way.

Let $\mathcal{M}_i = \{1,2,\cdots,M_i\}$, $1 \le i \le k$ be finite sets and let $\mathcal{M} = \prod_{i=1}^{k} \mathcal{M}_i$.

An $(n, M_1,\cdots,M_K)$ (symmetric alternating) k-user WUM code is a collection of sets $\mathscr{C} = \{C_u: u \in \mathcal{M}\}$ with $C_u \subset \{0,1\}^n$ such that, for all $u \in \mathcal{M}$ and all $v \in \mathcal{M}$ with $d_H(u,v) \le 1$ for all $x \in C_u$, a $y \in C_v$ exists with $x \wedge y = 0$.[1]

We consider the case $M_i = 2$ for $i = 1,\cdots,k$, and we address $[n,k]$ *one-bit* k-user WUM codes. Their total rate is obviously k/n.

[5, 3] *One-Bit WUM Code*:

$$C_{000} = \{00000\},\quad C_{100} = \{01100, 00011\},$$
$$C_{010} = \{01010, 00101\},\quad C_{001} = \{01001, 00110\},$$
$$C_{110} = \{00100, 10010\},\quad C_{101} = \{00001, 10100\},$$
$$C_{011} = \{00010, 10001\},\quad C_{111} = \{10000, 01000\}.$$

The rest of this section is devoted to a one-bit six-user WUM code. Its rate $\frac{6}{7}$ is surprisingly high for an alternating code.

[7, 6] *One-Bit WUM Code*: We first look at the point-line incidence matrix of a projective plane:

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

[1] Here and later, it is more convenient to denote sequences $z^n = (z_1,\cdots,z_n)$ by z.

Deleting the first column results in a 6×7 matrix:

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

Denote the entries of this matrix by z_{ij}; $1 \le i \le 6$, $1 \le j \le 6$; the rows by $X_1, X_2,\cdots, X_7$; and the columns by $Y_1, Y_2,\cdots, Y_6$. For $x \in \{0,1\}^6$, define

$$\Phi(x) \triangleq y = (y_1,\cdots,y_7)$$

where $y_i = 1$ iff $d_H(X_i, x) \le 2$ and $y_i = 0$ iff $d_H(X_i, x) \ge 3$. Similarly, for $y \in \Omega_3^7 = \{z \in \{0,1\}^7: |z| \le 3\}$, define

$$\Psi(y) \triangleq x = (x_1,\cdots,x_6)$$

where $x_i = 1$ iff $d_H(Y_i, y) \le 3$, $x_i = 0$ iff $d_H(Y_i, y) \ge 4$.

Theorem 6:

(i) $\Phi: \{0,1\}^6 \to \Omega_3^7$ is bijective and $\Psi = \Phi^{-1}$.

(ii) $\mathscr{C} = \{\{\Phi(x), \Phi(\bar{x})\}: x \in \{0,1\}^6\}$ is a one-bit six-user WUM code.

Ad (ii): We know from (i) that Φ is the encoding function and Ψ is the decoding function. Both functions are quite simple and easy to implement. Now, the WUM property remains to be verified. It suffices to show that $d_H(x,x') \le 1$ implies $\Phi(x) \wedge \Phi(\bar{x}') = 0$. For this, notice that in case $d_H(x,\bar{x}') \ge 5$ for any i, we have, by the triangle inequality, either $d_H(x, X_i) \ge 3$ or $d_H(\bar{x}', X_i) \ge 3$. This means that

$$(\Phi(x) \wedge \Phi(\bar{x}'))_i = 0 \quad \text{for } i = 1,2,\cdots,n$$
$$\text{or} \quad \Phi(x) \wedge \Phi(\bar{x}') = 0.$$

IX. More Open Problems

Problem 7 (Carrier Problem): Prescribe cost function Φ, per-letter cost d, and rate R. Find $S \subset \mathcal{X}^n$ with minimal cardinality such that

$$\forall s \in S: |S \cap S_{dn}(s)| \ge \exp\{Rn\}$$

where $S_{dn}(s)$ = sphere of cost radius dn. In particular, we are interested in the Hamming case.

Problem 8: Recall from the Introduction the definition of an (n, M, d) WEM code in case (E_+, D_-), and for any code $\mathscr{C} = \{C_1,\cdots,C_M\}$, the definitions of $d_{\mathscr{C}}$, $\nu_{\mathscr{C}}$, and $R(d)$.

We impose the following condition on $\mathscr{C}$.

$$|C_i| \le \exp\{\rho n\} \qquad \text{for } i = 1,2,\cdots,M \qquad (9.1)$$

and set $R(d,\rho) = \sup\{\nu_{\mathscr{C}}: d_{\mathscr{C}} \le d, \mathscr{C} \text{ satisfies (9.1)}\}$. Determine this rate function. There is a relation to Problem 7.

Problem 9: We speak of an automatic privacy guarantee if the code $\{C_{ij}: 1 \le i \le M, 1 \le j \le N\}$ is such that updatings from C_{ij} to $C_{i'j'}$ in one step are impossible (for instance, for the WUM or other cost constraints) if $i \ne i'$ *and* $j \ne j'$. This means that the users can "move only in rows or columns," and keeping their interests in updating

never can hurt the other. What are the achievable rates in the various models of side information, etc.?

APPENDIX
TWO SINGLE-USER WUM CODES

We begin with historical remarks.

Write-unidirectional memories (WUM's) have been introduced independently by Willems and Vinck [3] and Borden [4]. A WUM is a binary storage medium that is constrained the the following way. During alternate updatings of its contents, the encoder may write either 1's in selected bit locations or 0's in selected bit locations, but is not permitted to write combinations of 0's and 1's. Such a constraint arises when the mechanism that chooses to write 0's or 1's operates much more slowly than that of accessing and scanning the memory.

Corresponding to the given constraint, a WUM code is defined as follows.

A family $\mathscr{C} = \{C_1, \cdots, C_M\}$ of subsets of $\{0,1\}^n$ is a *WUM code of length n and size M*, if

(i) $C_i \cap C_j = \varnothing$ for $i \neq j$,

(ii) for all $i \in \{1, \cdots, M\}$, all $x \in C_i$, and all $j \in \{1, \cdots, M\}$, there exists a vector $y \in C_j$ such that $x \leq y$ or $y \leq x$, where we write $x = (x_1, \cdots, x_n) \leq y = (y_1, \cdots, y_n)$ if, for all $i = 1, \cdots, n$, $x_i = 1$ implies $y_i = 1$.

The sets C_i are called the *WUM sets* of the code $\mathscr{C}$. All codewords of a set C_i represent the same message, say m_i. We use the abbreviation (n, M) code for a WUM code of length n and size M. The rate R of an (n, M) code is

$$R = \frac{1}{n} \log_2 M. \tag{A.1}$$

Let $M(n)$ be the maximum value of M such that there exists an (n, M) code, and let $R(n)$ be the corresponding rate. Borden [4] proved the following result.

Theorem:

$$\text{(i)} \quad R(n) < \gamma := \log_2 \left(\frac{1 + \sqrt{5}}{2} \right) \approx 0.6942 \qquad \text{if } n \geq 5 \tag{A.2}$$

$$\text{(ii)} \quad \lim_{n \to \infty} R(n) = \gamma. \tag{A.3}$$

In Borden's model, the encoder can choose whether he will operate in the 0-write state or in the 1-write state when he updates the information stored by the WUM. Willems and Vinck considered a slightly different model. They required that the encoder writes 0's and 1's alternately during successive updatings. The WUM code in the sense of Willems and Vinck has later been called alternating WUM code by Simonyi [5]. Its definition is given in Section IV.

Let $R_a(n)$ be the maximal rate of an alternating WUM code of length n. It follows from Borden's proof of his theorem above that also $\lim_{n \to \infty} R_a(n) = \gamma$. The subclass of alternating WUM codes is important because any alternating WUM code can be expanded with the same rate to arbitrarily large n simply by concatenation. Note that this is not true for general WUM codes.

Borden's proof of (A.3) is not constructive. The best explicit construction in [4] for arbitrarily large n yields $R = \frac{1}{2}$ and is the following one. Let n, the number of binary positions of the memory, be even, and assume that the memory is initially filled with 0's. Divide the WUM into two parts, A and B, each of size $n/2$. When updating the content of the memory for the first time, write 1's in selected bit locations of part A and in all bit locations of part B of the memory; during the next updating, write 0's into all bit locations of part A and into selected bit locations of part B, and so on. Thus, in every updating, $n/2$ bits of information can be stored in one of the two parts of the memory, and the other part is prepared for the next updating. This corresponds to a WUM code with the rate $R_n = \frac{1}{2}$.

Several WUM codes with higher rates are know. Willems and Vinck [3] gave the construction of a (5,6) code with the rate $(\log_2 6)/5 \approx 0.5170$. Simonyi [5] presented an (11,58) code with the rate $(\log_2 58)/11 \approx 0.5325$. Zhang constructed the (10,41) code and the (15,307) code presented below which achieve the rates 0.5376 and 0.5508, respectively. The presently known highest rate is 0.5637 for Koschnick's [11] (17,767) code. All of these codes have the "alternating" property, and therefore can be used for arbitrarily large memories.

They are also all symmetric in the sense defined in (4.3).

To fix ideas, we begin with a simple symmetric alternating WUM code.

Example—(5, 6) WUM code (Willems and Vinck [3]):

$$C_1 = \{10000, 01100, 00011\}, \quad C_2 = \{01000, 10010, 00101\},$$

$$C_3 = \{00100, 10001, 01010\}, \quad C_4 = \{00010, 10100, 01001\},$$

$$C_5 = \{00001, 11000, 00110\}, \quad C_6 = \{00000\}.$$

The rate of this code is $\frac{1}{5} \log_2 6 \approx 0.5170$.

This code, as well as Simonyi's code, have the property that for all $i \in \{1, \cdots, M\}$, the words of the WUM sets C_i have disjoint supports. However, one can show that symmetric alternating WUM codes with this property cannot have rates arbitrarily near γ. Actually, the best code with this property is Simonyi's code having the rate 0.5325.

We now present two single-user WUM codes. One of them is a (10,41) code; the other one is a (15,307) code. We first introduce a new concept—WUM subsets—which will play a key role in their constructions.

Let

$$\Omega_k^n = \{x \in \{0,1\}^n : \|x\| \leq k\} \tag{A.4}$$

where $\|x\|$ is the weight of x.

A subset W of Ω_k^n is called an (n, k) WUM set if

$$\forall x \in \Omega_k^n \quad \exists y \in W \quad \text{such that } y \text{ and } x \text{ are disjoint.} \tag{A.5}$$

Obviously, a set of disjoint (n, k) WUM subsets of Ω_k^n for a symmetric alternating WUM code. Our two codes presented here are both of this type.

First, the reader is asked to check that the following sets are (10,3) WUM sets.

A:	B:	C:
1110000000	1110000000	1110000000
1101000000	0001110000	0001110000
0011000000	0000001110	0000001100
0000111000	0000000001;	0000000011.
0000000111;		

Not only are these three sets (10,3) WUM sets, but their permutations are as well. In fact, we have the following more general *observation*:

Let W be an (n, k) WUM set and π a permutation on the set $\{1, \cdots, n\}$; then πW is again an (n, k) WUM set.

Now, the idea for our construction is clear. To construct our codes, we first choose a set of basic WUM sets, and then choose a set of permutations for each WUM set to make the results of

the permutations all disjoint. These WUM sets obtained from the permutations form a WUM code. An inspection of Borden's proof of (A.2) shows that rates arbitrarily close to γ can be obtained with these codes. The task of choosing WUM sets and permutations is usually very difficult. It can be done (as here) artistically or algorithmically (as in [11]).

(10, 41) WUM Code: We use the following permutation in the construction of this code:

$$s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 3 & 4 & 5 & 1 & 7 & 8 & 9 & 10 & 6 \end{pmatrix}.$$

This permutation has the property that

$$s^5 = I,$$

and for any nonzero codeword x in Ω_3^{10}, $sx \neq x$. To show how this permutation works on the words in $\{0,1\}^{10}$, we present the following example.

Let

$$x = 1101001010;$$

then

$$sx = 0110100101, \quad s^2x = 1011010010,$$

$$s^3x = 0101101001, \quad s^4x = 1010110100,$$

and finally,

$$s^5x1101001010 = x.$$

For a set A of words, s^iA is defined by $s^iA = \{s^ix: x \in A\}$.

The (10, 41) WUM code consists of the set {0000000000}, and the following eight basic WUM subsets B_1–B_8 of Ω_3^{10} and all their permutations s^iB_j $0 \le i \le 4$, $1 \le j \le 8$. There are all together $1 + 5 \times 8 = 41$ distinct subsets in this code. We leave to the reader the task to check that this code satisfies all of the requirements for a symmetric alternating WUM code. This can be done by computer.

B_1: 1100010000
1100001000
0000011000
0010100010
0001000101

B_2: 1010010000
1010000100
0000010100
0001101000
0100000011

B_3: 1000011000
0100011000
1100000000
0011000001
0000100110

B_4: 0010000010
00010000100
0000111000
1100000001

B_5: 0001010100
1000001010
0000000001
0110100000

B_6: 1010000010
0101010000
0000100000
0000001101

B_7: 1000010100
0001001010
0100000001
0010100000

B_8: 1110000000
0000001110
0000100001
0001010000

(15, 307) WUM Code: This code uses up all of the words in Ω_4^{15}. It consists only of (15, 4) WUM sets. To describe the construction of this code, we first introduce a few basic permutations:

$$S = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 2 & 3 & 4 & 5 & 1 & 7 & 8 & 9 & 10 & 6 & 12 & 13 & 14 & 15 & 11 \end{pmatrix};$$

$$S_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 2 & 3 & 4 & 5 & 1 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \end{pmatrix};$$

$$S_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 1 & 2 & 3 & 4 & 5 & 7 & 8 & 9 & 10 & 6 & 11 & 12 & 13 & 14 & 15 \end{pmatrix};$$

$$S_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 12 & 13 & 14 & 15 & 11 \end{pmatrix};$$

$$T = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 11 & 12 & 13 & 14 & 15 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix};$$

$$R = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 6 & 7 & 8 & 9 & 10 & 1 & 2 & 3 & 4 & 5 & 11 & 12 & 13 & 14 & 15 \end{pmatrix}.$$

The code contains the set {000000000000000}, and the following 12 basic WUM sets and their various permutations. The 12 basic sets are

A_1: 110001000001000
010001100010000
100000100011000
001010010000001
000010010100100
001000000100101
000100001000010;

A_2: 110001100000000
000001100011000
110000000011000
001100000100000
000000011000001
000010000000110;

A_3: 101001010000000
000001010010100
101000000010100
010110000000000
000000101100000
000000000001011;

A_4: 101001000000000
000000101001000
000010000010010
010010000100000
000000010000101;

A_5: 110000001000000
000001100001000
000100000010100
000000010100001
001010000000010;

A_6: 111001000000000
110100010000000
001101010000000
000010000010100
000000101100001
000000001001011
000000100101010;

A_7: 111000001000000
110100000100000
001100001100000
000010000011000
000001110000100
000000100000111
000001010000011;

A_8: 000010000000000
111000100000000
000100011100000
000001000000001
000000000011110;

A_9: 110001010000000
000001010001010
110000000001010
000000101010100
000000100110001
000000001100101
001110000000000;

A_{10}: 101000110000000
000001000110100
000110000000010
000000001001000
010000000000001;

A_{11}: 110000011000000
000001000100110
000000100010001
001000000001000
000110000000000;

A_{12}: 110100001000000
000010110100000
001000000000110
000001000010000
000000000001001.

The (15, 307) WUM code consists of the following subsets of Ω_4^{15}:

a) {000000000000000};
b) $S_1^i S_2^j S_3^k A_1$, $0 \le i \le 4$, $0 \le j \le 4$, $0 \le k \le 4$;
c) $S^i A_j$, $0 \le i \le 4$, $2 \le j \le 3$;
d) $T^i R^j A_4$, $0 \le i \le 2$, $0 \le j \le 1$;
e) $S^i T^j R^k A_l$, $0 \le i \le 4$, $0 \le j \le 2$, $0 \le k \le 1$, $5 \le l \le 7$;
f) $S^i T^j A_l$, $0 \le i \le 4$, $0 \le j \le 2$, $8 \le l \le 12$.

Remark: For these two codes, only minimal WUM sets and all the elements in Ω_k^n are used. This leads us to conjecture that these two codes are optimal for their blocklengths.

REFERENCES

[1] A. V. Kuznetsov and B. S. Tsybakov, "Coding in a memory with defective cells," *Prob. Inform. Transmission*, vol. 10, no. 2, pp. 132–138, 1974.

[2] R. Ahlswede and Z. Zhang, "Coding for write-efficient memory," *Inform. Computation*, vol. 83, no. 1, pp. 80–97, 1989.

[3] F. M. J. Willems and A. J. Vinck, "Repeated recording for an optical disk," in *Proc. 7th Symp. Inform. Theory in the Benelux*, May 1986, Delft Univ. Press, pp. 49–53.

[4] J. M. Borden, "Coding for write-unidirectional memories," submitted to *IEEE Trans. Inform. Theory*.

[5] G. Simonyi, "On write-unidirectional memory codes," *IEEE Trans. Inform. Theory*, pp. 663–667, May 1989.

[6] R. Ahlswede, N. Cai, and Z. Zhang, "A new direction in extremal theory for graphs," *J. Combinatorics, Information & System Sciences*, to be published.

[7] ——, "Diametric theorems in sequence spaces," *Combinatorica*, vol. 12, no. 1, pp. 1–17, 1992.

[8] ——, "Rich hypergraph colorings with local constraints," SFB 343 "Diskrete Strukturen in der Mathematik," Bielefeld, Germany, Preprint 89-011, 1989; *J. Combinatorics, Information & System Sciences*, vol. 17, Nos. 3–4, pp. 203–216, 1992.

[9] G. Cohen, "On the capacity of write-unidirectional memories," *Bull. Inst. Math. Acad. Sinica*, vol. 16, no. 4, pp. 285–293, 1988.

[10] F. M. J. Willems, "Converses for write-unidirectional memories," EUT Rep. 89-E-220.

[11] K. U. Koschnick, "Good code design with combinatorial approximation algorithms," Dissertation, Bielefeld, Germany, 1990.

[12] R. Ahlswede and G. Simonyi, "Reusable memories in the light of the old AV- and a new F-channel theory," *IEEE Trans. Inform. Theory*, vol. 37, no. 4, pp. 1143–1150, 1991.

[13] R. L. Rivest and A. Shamir, "How to use a write-once memory," *Inform. Contr.*, vol. 55, pp. 1–19, 1982.

[14] J. K. Wolf, A. D. Wyner, J. Ziv, and J. Körner, "Coding for write-once memory," *AT & T. Tech. J.*, vol. 63, no. 6, pp. 1098–1112, 1984.

[15] R. Ahlswede, "Coloring hypergraphs: A new approach to multi-user source coding, Part I, II," *J. Combinatorial Inform. Syst. Sci.*, vol. 4, pp. 76–115; no. 5, pp. 220–268, 1979/1980.

[16] R. Ahlswede and I. Althöfer, "The asymptotic behavior of diameters in the average," SFB 343 "Diskrete Strukturen in der Mathematik," Bielefeld, Germany, Preprint 91-099, 1991; *J. Combinatorial Theory*, to be published.

[17] R. Ahlswede, N. Cai, and Z. Zhang, "Higher level extremal problems," SFB 343 "Diskrete STrukturen in der Mathematik," Bielefeld, Germany, Preprint 92-031, 1992; submitted to *J. Combinatorics, Information & System Sciences*.

[18] R. Ahlswede and G. Dueck, "Identification via channels," *IEEE Trans. Inform. Theory*, vol. 35, pp. 15–29, 1989.

[19] ——, "Identification in the presence of feedback—A discovery of new capacity formulas," *IEEE Trans. Inform. Theory*, vol. 35, pp. 30–36, 1989.

[20] R. Ahlswede and N. Cai, "Models of multi-user write-efficient memories and general diametric theorems," SFB 343 "Diskrete Strukturen in der Mathematik," Bielefeld, Preprint 93-019, 1993; presented at the 6th Joint Swedish–Russian Int. Workshop Inform. Theory, Mölle, Sweden, Aug. 1993; submitted to *Information and Computation*.

[21] M. Salehi and F. M. J. Willems, "Ring source- and channel codes," in *Proc. 12th Symp. Inform. Theory*, Benelux, 1991, pp. 113–120.