DIMACS Series in Discrete Mathematics
and Theoretical Computer Science

# Unbounded Loss in Writing on Dirty Paper is Possible

Aaron S. Cohen and Ram Zamir

ABSTRACT. For a generalization of Costa's writing on dirty paper with irregular additive noise distribution, we show that the loss between the zero-interference capacity and the causal side information capacity can be arbitrarily large. This contrasts to the Gaussian noise case, where the capacity loss is zero or at most 1/4 bit for the non-causal and causal side information cases, respectively. This also contrasts to the bounded loss in the "dual" problem of rate distortion with side information.

## 1. Introduction

We consider a generalization of Costa's writing on dirty paper [**Cos83**], in which a channel has two independent sources of additive noise. The first source, $S^n$, is known to the transmitter and is referred to as "side information" or "interference". The second source, $Z^n$, is not directly known to any part of the communication system. The input $X^n$ and the output $Y^n$ are related as $Y^n = X^n + S^n + Z^n$.

Here, we fix constants $\alpha$ and $L$ and a set $A_z \subset \{1, \ldots, L\}$. The noise sources are i.i.d. with $Z_i$ uniformly distributed over $A_z$ and $S_i$ uniformly distributed over $\{1, \ldots, L\}$, which refer to as "strong interference". Each input symbol $X_i$ is restricted to $\{1, \ldots, \alpha\}$. All arithmetic is done modulo $L$ with results in $\{1, \ldots, L\}$.

We write the capacity of this channel as $C_{\mathrm{C}}(\alpha, L, A_z)$ or $C_{\mathrm{NC}}(\alpha, L, A_z)$ depending on whether the transmitter side information can be used causally (i.e., $X_k$ can depend only on $S_1, \ldots, S_k$) or non-causally (i.e., the input sequence $X^n$ depends on the entire side information sequence $S^n$). The causal version is sometimes referred to as "writing on dirty tape". Our main result compares the causal case to the zero-interference case, where the output is given by $Y^n = X^n + Z^n$ and the capacity is denoted by $C_{\mathrm{ZI}}(\alpha, L, A_z)$. The zero-interference case is equivalent to both the transmitter and receiver having access to the side information (either causally or non-causally). See Section 2 for the definitions of the capacities.

THEOREM 1.1. *The capacity loss between the zero-interference case and the causal side information case is potentially unbounded. That is, for any $\Delta > 0$,*

---

1991 *Mathematics Subject Classification.* Primary 94A24; 05A99.
*Key words and phrases.* Channels with Side Information, Rate Loss, Capacity.
A. Cohen supported in part by the National Science Foundation under Grant DMS-0074276.
R. Zamir supported in part by the Israel Science Foundation.

*there exists a modulo-additive noise channel with parameters $\alpha$, $L$, and $A_z$ such that* $C_{ZI}(\alpha, L, A_z) - C_C(\alpha, L, A_z) > \Delta$.

This result contrasts with the uniform bound on the rate loss per degree of freedom in the Wyner-Ziv problem, relative to common fidelity criteria such as the $r$th-power distortion measure [**Zam96, Zam02**]. Duality between such rate distortion with side information problems and input constrained communication with side information problems like writing on dirty paper has been the subject of several recent research efforts [**CC02, BCW03, PCR03**]. However, this result indicates that this duality is potentially not complete.

This result also contrasts with Costa's writing on dirty paper result [**Cos83**] of no loss for Gaussian noise and side information and a power constraint, albeit for the non-causal case. For the causal version of Costa's problem, the loss is bounded by the shaping gain (at most 1/4 bit) [**ESZ00, ESZ02**]. We also see the importance of the necessary conditions of no loss (in the non-causal case) for generalized writing on dirty paper [**CL02**]. The unboundedness of the loss in the non-causal case is addressed in [**CZ03b**]. In the remainder of this paper, we prove Theorem 1.1.

## 2. Capacities

The capacity is the largest rate at which reliable communication is achievable. For example, a rate $R$ is achievable in the zero-interference case if we can construct sequences (as $n = 1, 2, \dots$) of rate $R$, blocklength $n$ encoders, $f_n : \{1, \dots, 2^{nR}\} \mapsto \{1, \dots, \alpha\}^n$, and decoders, $g_n : \{1, \dots, L\}^n \mapsto \{1, \dots, 2^{nR}\}$, such that $\Pr(g_n(f_n(W) + Z^n) \neq W) \to 0$ as $n \to \infty$ for $W$ uniformly distributed on $\{1, \dots, 2^{nR}\}$. For the causal side information case, a blocklength-$n$ encoder consists of a sequence (as $k = 1, \dots, k$) of functions,

$$\left\{ f_{n,k} : \{1, \dots, 2^{nR}\} \times \{1, \dots, L\}^k \mapsto \{1, \dots, \alpha\}, 1 \leq k \leq n \right\}, \tag{2.1}$$

where $f_{n,k}$ produces the $k$th input $X_k$ from the entire message $W$ and the first $k$ side information values. The capacity for the causal side information case is otherwise the same as for the zero-interference case.

**2.1. Zero-Interference.** In this case, the capacity is given by

$$C_{\mathrm{ZI}}(\alpha, L, A_z) = \max_{P_X} I(X; X + Z), \tag{2.2}$$

where the maximum is over all distributions on $\{1, \dots, \alpha\}$ and the random variable $Z$ is independent of $X$ and uniformly distributed over $A_z$. Here, $I(X; Y)$ is the mutual information between random variables $X$ and $Y$, which can be written as a difference of entropies, $I(X; Y) = H(X) - H(X|Y) = H(Y) - H(Y|X)$. The entropy of the random variable $X$ with distribution $P$ is defined by $H(X) = -E[\log P(X)] = -\sum_x P(x) \log P(x)$.

We now give a condition on $A_z$ that results in the maximum possible capacity.

LEMMA 2.1. *If $A_z$ satisfies*

$$|z_1 - z_2| \geq \alpha, \ \ \forall z_1, z_2 \in A_z, \ z_1 \neq z_2, \tag{2.3}$$

*then* $C_{ZI}(\alpha, L, A_z) = \log \alpha$.

PROOF. First, note that $C_{\mathrm{ZI}}(\alpha, L, A_z) \leq \log \alpha$ since the transmitter can send one of $\alpha$ values at each time (also since $I(X; Z) \leq H(X) \leq \log \alpha$). However, the decoder can exactly recover any transmitted sequence since the values in $A_z$ are separated by at least $\alpha$. More technically, if we let $P_X$ be uniform over $\{1,\ldots,\alpha\}$, then (2.3) implies that $\Pr(X+Z=j)$ is $\frac{1}{\alpha|A_z|}$ for $\alpha|A_z|$ values of $j$. Thus, the mutual information of interest, which can be written $I(X;X+Z)=H(X+Z)-H(X+Z|X)=H(X+Z)-H(Z)$, is $\log\alpha|A_z|-\log|A_z|=\log\alpha$. □

**2.2. Causal Side Information.** In [**Sha58**], Shannon developed a general formula for capacity with causal side information. This formula involves maximizing over distributions of functions from the side information space to the input space (here, this would be functions from $\{1,\ldots,L\}$ to $\{1,\ldots,\alpha\}$, and there are $\alpha^L$ such functions). In [**ESZ00, ESZ02**], the capacity optimization is simplified for the important case of additive noise and strong interference (e.g., for $S$ uniform over $\{1,\ldots,L\}$). By further imposing a hard input constraint, we see that

$$C_{\mathrm{C}}(\alpha,L,A_z)=\log L-\min_{t:\{1,\ldots,L\}\to\{1,\ldots,\alpha\}}H(t(S)+S+Z). \tag{2.4}$$

This formula only requires an optimization over the $\alpha^L$ functions $t(\cdot)$ from the side information space to the input space, *not* the distributions over such functions.

## 3. Lower Bounding The Loss

In this section, we prove Theorem 1.1 by lower bounding the difference between the zero-interference capacity and the causal capacity. In Section 3.1, we develop a general lower bound on the entropy of $t(S)+S+Z$. We refer to this random variable as the *effective noise* and denote its probability mass function (PMF) by $\boldsymbol{p}^{\mathrm{eff}}=\boldsymbol{p}^{\mathrm{eff}}(t(\cdot),A_z,L)$. This distribution can be expressed in terms of the sets

$$C_j=\{1\le s\le L\ :\ j-t(s)-s\in A_z\},\quad \forall 1\le j\le L. \tag{3.1}$$

The set $C_j$ consists of the side information values $s$ that contribute to the distribution of the effective noise at $j$ since $s\in C_j$ implies that $t(s)+s+z=j$ for some $z\in A_z$. Indeed, since $S$ is uniformly distributed over $\{1,\ldots,L\}$ and $Z$ is uniformly distributed over $A_z$, we have that

$$p_j^{\mathrm{eff}}=\Pr(t(S)+S+Z=j)=\frac{|C_j|}{L|A_z|},\quad \forall 1\le j\le L. \tag{3.2}$$

In Section 3.2, we upper bound the number of sets $C_j$ that can be large (and hence the number of values of $p_j^{\mathrm{eff}}$ that can be large) using the size of the intersection of $A_z$ with a shifted version of itself. In Section 3.3, we construct a set $A_z$ that satisfies (2.3) yet has a small self intersection. In Section 3.4, we complete the proof by combining the previous steps.

**3.1. Majorization Bound on Entropy.** We first consider the points in the PMF of the effective noise that are relatively large. For $0\le\beta\le L$, define the set

$$J(\beta,t,A_z,L)=\left\{j\ :\ p_j^{\mathrm{eff}}\ge\beta/L\right\}. \tag{3.3}$$

Clearly, we must have $|J(\beta,t,A_z,L)|\le L/\beta$. The next lemma uses a majorization argument assuming that, for some $\beta<\alpha$, we have $|J(\beta,t,A_z,L)|\le L/\alpha$.

LEMMA 3.1. *For any $\beta<\alpha$ with $|J(\beta,t,A_z,L)|\le L/\alpha$,*

$$H(t(S)+S+Z)\ge|J(\beta,t,A_z,L)|\frac{\alpha}{L}\log\frac{L}{\alpha}+\Big(1-|J(\beta,t,A_z,L)|\frac{\alpha}{L}\Big)\log\frac{L}{\beta}. \tag{3.4}$$

PROOF. For simplicity we write $J$ for $J(\beta, t, A_z, L)$ during the course of the proof. Consider the PMF $\boldsymbol{p}^*$ on the L-dimensional simplex defined as

$$\boldsymbol{p}^* = \Big[\underbrace{\frac{\alpha}{L}, \frac{\alpha}{L}, \ldots, \frac{\alpha}{L}}_{|J| \text{ times}}, \underbrace{\frac{\beta}{L}, \frac{\beta}{L}, \ldots, \frac{\beta}{L}}_{\left\lfloor \frac{L-|J|\alpha}{\beta} \right\rfloor \text{ times}}, \ \xi, \ 0, \ldots, 0\Big], \tag{3.5}$$

where $\xi \le \beta/L$ is chosen so that $\sum_{j=1}^{L} p_j^* = 1$. The PMF $\boldsymbol{p}^*$ majorizes the PMF $\boldsymbol{p}^{\text{eff}}$, written $\boldsymbol{p}^{\text{eff}} \prec \boldsymbol{p}^*$; see [**MO79**] for the definition of majorization and the results below. To see this, first note that $p_j^{\text{eff}} \le \frac{\alpha}{L}$ since $|C_j| \le \alpha|A_z|$ for all $j$; see (3.1) and (3.2). Thus, the sum of the largest $k \le |J|$ components of $\boldsymbol{p}^{\text{eff}}$ cannot exceed $\frac{k\alpha}{L}$. Next, from the definition of $J(\beta, t, A_z, L)$ note that only $|J|$ components of $\boldsymbol{p}^{\text{eff}}$ can exceed $\frac{\beta}{L}$. Thus, the sum of the largest $k > |J|$ components cannot exceed $\frac{|J|\alpha + (k-|J|)\beta}{L}$ or 1, whichever is smaller. These two properties insure that the sum of the largest $k$ components of $\boldsymbol{p}^{\text{eff}}$ cannot exceed the sum of the largest $k$ components of $\boldsymbol{p}^*$, which is precisely the definition of majorization. Since entropy is Schur-concave, we can conclude that $H(\boldsymbol{p}^{\text{eff}}) \ge H(\boldsymbol{p}^*)$. We complete the proof by lower bounding the entropy of $\boldsymbol{p}^*$

$$H(\boldsymbol{p}^*) = |J|\frac{\alpha}{L}\log\frac{L}{\alpha} + \left\lfloor \frac{L-|J|\alpha}{\beta} \right\rfloor \frac{\beta}{L}\log\frac{L}{\beta} + \xi\log\frac{1}{\xi} \tag{3.6}$$

$$\ge |J|\frac{\alpha}{L}\log\frac{L}{\alpha} + \Big(1 - |J|\frac{\alpha}{L}\Big)\log\frac{L}{\beta}. \tag{3.7}$$

□

**3.2. Combinatorial Bound on Effective Noise Distribution.** We next define a function related to the auto-correlation of the actual noise distribution,

$$M(n, A_z) = |A_z \cap (A_z + n)|. \tag{3.8}$$

Here, $A_z + n = \{a + n : a \in A_z\}$. We upper bound $|J(\beta, t, A_z, L)|$ using

$$M^*(A_z) = \max_{n \ne 0} M(n, A_z). \tag{3.9}$$

LEMMA 3.2. *For any $\beta$ with $\sqrt{\alpha M^*(A_z)L/|A_z|^2} < \beta < \alpha$ and for all functions $t(\cdot)$,*

$$|J(\beta, t, A_z, L)| \le \frac{\beta|A_z| - \alpha M^*(A_z)}{\frac{(\beta|A_z|)^2}{L} - \alpha M^*(A_z)}. \tag{3.10}$$

PROOF. We shall again write $J$ for $J(\beta, t, A_z, L)$ in this proof. The intersection of two $C_j$'s can be written as

$$C_j \cap C_{j'} = \{1 \le s \le L \ : \ j - s - t(s) \in A_z \cap (A_z + j - j')\}; \tag{3.11}$$

compare with (3.1). This follows since $s \in C_j \cap C_{j'}$ only if $j - s - t(s) \in A_z$ *and* $j' - s - t(s) \in A_z$, and the latter is equivalent to $j - s - t(s) \in (A_z + j - j')$. Since the function $t(\cdot)$ only takes on $\alpha$ different values, we can bound the size of the intersection by

$$|C_j \cap C_{j'}| \le \alpha M^*(A_z), \ \ \forall j \ne j'; \tag{3.12}$$

see (3.8), (3.9), and (3.11). We also see that

$$|C_j| \ge \beta|A_z|, \ \ \forall j \in J; \tag{3.13}$$

see (3.2) and (3.3). We use these bounds to give a combinatorial proof of the lemma.

Let us define $\gamma(s) = |\{j \in J \, : \, s \in C_j\}|$ and $\bar{\gamma} = L^{-1}\sum_{s=1}^{L}\gamma(s)$. That is, $\gamma(s)$ is the number of members of $J$ for which $s$ contributes to the PMF of the effective noise. We first observe that $\sum_{s=1}^{L}\gamma(s) = \sum_{j\in J}|C_j|$, since both sums are counting the same objects. Thus, the average value can be lower bounded using

$$\bar{\gamma} = L^{-1}\sum_{s=1}^{L}\gamma(s) = L^{-1}\sum_{j\in J}|C_j| \geq \frac{\beta|J||A_z|}{L}, \tag{3.14}$$

where we have used (3.13) above. A similar counting argument for pairs of elements gives $\sum_{s=1}^{L}\binom{\gamma(s)}{2} = \sum_{j\neq j'\in J}|C_j \cap C_{j'}|$. Therefore,

$$\frac{\bar{\gamma}(\bar{\gamma}-1)}{2} \leq L^{-1}\sum_{s=1}^{L}\binom{\gamma(s)}{2} = L^{-1}\sum_{j\neq j'\in J}|C_j\cap C_{j'}| \leq \binom{|J|}{2}\frac{\alpha M^*(A_z)}{L}, \tag{3.15}$$

where the first bound follows from Jensen's inequality since $x(x-1)/2$ is convex in $x$ and the second bound follows by (3.12) since there are $\binom{|J|}{2}$ pairs of elements in the set $J$. The combination of the bounds (3.14) and (3.15) under the condition given in the lemma gives (3.10), and the proof is complete. □

**3.3. Construction of $A_z$ Using Arithmetic Differences.** We next construct a set $A_z$ and give an upper bound on $M^*(A_z)$ for this $A_z$. The main idea is to find a set $A_z$ in which (2.3) is satisfied (so that $C_{\mathrm{ZI}}(\alpha, A_z, L)$ is large) and yet the maximum autocorrelation $M^*(A_z)$ is small (so that $C_{\mathrm{C}}(\alpha, A_z, L)$ is small). Before giving our construction, we consider some other possibilities. The set cannot be periodic, since $M^*(A_z)$ would then be large. For example, if $A_z = \{\alpha, 2\alpha, \ldots, \lfloor L/\alpha\rfloor\alpha\}$, then $M^*(A_z) \geq |A_z| - 1$ which is practically the maximum value. Another possibility could be to let $A_z$ be a subset of the exponential series $\{2^k; k = 1, 2, \ldots\}$, which results in the minimal $M^*(A_z) = 1$. However, the size of any such set grows as $\log L$ and the denominator (3.10) would not grow to infinity. A final possibility could be to find a set $A_z$ so that $M(n, A_z) = 1$ for *all* non-zero $n$, while the size of $A_z$ grows as $\sqrt{L}$. Such a set (known as a planar difference set) exists for all $L = p^k + 1$, where $p$ is a prime and $k$ is an integer [**BJL99**]. A planar difference set minimizes $M^*(A_z)$ for fixed $L$ and $|A_z|$, but does not necessarily satisfy (2.3); see [**CZ03b**] for the use of difference sets in this problem.

To construct our $A_z$, we let $L = (2\alpha - 1)^2$ and let

$$A_z = \left\{\sum_{k=1}^{j}\alpha + k - 1 \; : \; 0 \leq j < 2\alpha - 1\right\}. \tag{3.16}$$

For example, if $\alpha = 3$, then $A_z = \{3, 7, 12, 18, 25\}$. We refer to this $A_z$ as an *arithmetic difference sequence* since the difference between the $j$th and $(j+1)$st points in $A_z$ is $\alpha + j - 1$. We thus see that (2.3) is satisfied. Note that for every $z \in A_z \cap (A_z + n)$, there exists integers $j_1$ and $j_2$ such that either $n$ or $L - n$ can be represented as $\sum_{k=j_1+1}^{j_2}\alpha + k - 1 = (j_2 - j_1)(2\alpha + j_1 + j_2 - 1)/2$. In other words, the size of $A_z \cap (A_z + n)$ is related to the number of factorizations of $n$ and $L - n$. Let $d(n)$ be the number of factors of $n$ (e.g., $d(4) = 3$, $d(5) = 2$, $d(6) = 4$). This reasoning gives the following result.

LEMMA 3.3. *For any $\alpha$, if $L = (2\alpha - 1)^2$ and $A_z$ is defined as in (3.16), then*

$$M(n, A_z) \le \frac{d(n) + d(L-n)}{2}, \ \forall 1 \le n \le L. \tag{3.17}$$

*Consequently, $M^*(A_z) \le \max_{1 \le n \le L} d(n)$.*

The final step is to bound the growth of $M^*(A_z)$ as a function of $\alpha$. (Note that it is necessary to let $\alpha$ grow to infinity in order for the loss to become unbounded.) A sufficient bound on the growth is given by the following number theoretic result on the number of divisors.

LEMMA 3.4. [**HW79**, Theorem 315] *For any $\delta > 0$, $\lim_{n \to \infty} d(n)/n^{\delta} = 0$.*

**3.4. Combining the Bounds.** For any $\beta$ and $A_z$ such that the conditions in Lemmas 3.1 and 3.2 are satisfied, we see that

$$C_{\mathrm{ZI}}(\alpha, L, A_z) - C_{\mathrm{C}}(\alpha, L, A_z) \ge \max_{t(\cdot)} \left(1 - |J(\beta, t, A_z, L)| \frac{\alpha}{L}\right) \log \frac{\alpha}{\beta} \tag{3.18}$$

$$\ge \left(1 - \frac{\beta |A_z| - \alpha M^*(A_z)}{\frac{(\beta |A_z|)^2}{L} - \alpha M^*(A_z)} \frac{\alpha}{L}\right) \log \frac{\alpha}{\beta} \tag{3.19}$$

where (3.18) follows by Lemma 3.1 and (3.19) follows by Lemma 3.2. So far, we have not used the arithmetic difference sequence $A_z$. For this $A_z$, we can write the relevant parameters as functions of $\alpha$. In particular, we have that $L = (2\alpha - 1)^2$, $|A_z| = (2\alpha - 1) = \sqrt{L}$, and that (from Lemmas 3.3 and 3.4) $M^*(A_z) = o(\alpha^{2\delta})$ for any positive $\delta$. Thus, for any $1/2 < \lambda < 1$, let $\beta = \alpha^{\lambda}$ and the bound becomes

$$C_{\mathrm{ZI}}(\alpha, L, A_z) - C_{\mathrm{C}}(\alpha, L, A_z)$$

$$\ge \left(1 - \frac{\alpha^{\lambda}(2\alpha - 1) - \alpha M^*(A_z)}{\alpha^{2\lambda} - \alpha M^*(A_z)} \frac{\alpha}{(2\alpha - 1)^2}\right) (1 - \lambda) \log \alpha \tag{3.20}$$

$$= (1 - \lambda) \log \alpha + o(\log \alpha), \tag{3.21}$$

where the asymptotics follow since $M^*(A_z)$ is $o\left(\alpha^{2\lambda - 1}\right)$ and $o\left(\alpha^{\lambda}\right)$ for all $\lambda > 1/2$. Thus, the big fraction grows as $\alpha^{-\lambda}$ which tends to zero as $\alpha$ grows to infinity. This completes the proof of the theorem since we can choose $\alpha$ arbitrarily large.

## 4. Conclusions

We have shown that the the capacity with causal side information at the transmitter can be arbitrarily smaller than the capacity with side information at both the transmitter and receiver. Indeed, for the arithmetic difference sequence $A_z$ (3.16), we have asymptotically upper bounded $C_{\mathrm{C}}(\alpha, L, A_z)/C_{\mathrm{ZI}}(\alpha, L, A_z)$ by 1/2.

In [**CZ03a, CZ03b**], we strengthen these results in several ways. First, we extend the capacity analysis to the non-causal case. In particular, we show that the non-causal capacity is given by

$$C_{\mathrm{NC}}(\alpha, L, A_z) = \max_{P_V} \left( H(V) - \min_{t:\{1,\ldots,L\} \to \{1,\ldots,\alpha\}} H(t(V) + V + Z) \right), \tag{4.1}$$

where the maximum is over distributions of the random variable $V$, which takes value on the set $\{1, \ldots, L\}$. Note that the right hand side of (4.1) is equal to the causal capacity (2.4) when $P_V$ is uniform over $\{1, \ldots, L\}$. Second, we show that if $A_z$ is a difference set, then the non-causal capacity is at most 2 bits/channel use, while the zero-interference capacity is at least $\log \alpha - 1$ bits/channel use for any constraint set of size $\alpha$. The minus one results from the fact that (2.3) is not satisfied all of the time. Thus, the rate loss can be arbitrarily large in the non-causal case as well. Furthermore, for both causal and non-causal cases, the ratio of capacity with side information to zero-interference capacity can be arbitrarily small. Finally, we would like to generalize our results to continuous alphabets and expected input constraints.

## Acknowledgments

The authors would like to thank Uri Erez, Dave Forney, Aaron Hoffman, Ishai Ilani, and Simon Litsyn for helpful comments and suggestions.

## References

[BCW03] Richard J. Barron, Brian Chen, and Gregory W. Wornell, *The duality between information embedding and source coding with side information and some applications*, IEEE Trans. Inform. Theory **49** (2003), no. 5, 1159–1180.

[BJL99] Thomas Beth, Dieter Jungnickel, and Hanfried Lenz, *Design theory*, second ed., vol. 1, Cambridge University Press, 1999.

[CC02] Mung Chiang and Thomas M. Cover, *Duality between channel capacity and rate distortion with two-sided state information*, IEEE Trans. Inform. Theory **48** (2002), no. 6, 1629–1638.

[CL02] Aaron S. Cohen and Amos Lapidoth, *Generalized writing on dirty paper*, Proc. of the Inter. Symposium on Info. Theory (Lausanne, Switzerland), 2002, p. 227.

[Cos83] Max H. M. Costa, *Writing on dirty paper*, IEEE Trans. Inform. Theory **29** (1983), no. 3, 439–441.

[CZ03a] Aaron S. Cohen and Ram Zamir, *The rate loss in writing on dirty paper*, In preparation, 2003.

[CZ03b] ———, *Writing on dirty paper in the presence of difference set noise*, Proc. of the Allerton Conf. on Comm., Control and Computing, 2003.

[ESZ00] Uri Erez, Shlomo Shamai, and Ram Zamir, *Capacity and lattice-strategies for cancelling known interference*, Proc. of the Inter. Symposium on Info. Theory and its Applications (Honolulu, HI), 2000, pp. 681–684.

[ESZ02] ———, *Capacity and lattice-strategies for cancelling known interference*, Submitted to *IEEE Trans. Info. Theory*, 2002.

[HW79] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, fifth ed., Oxford, Clarendon, 1979.

[MO79] Albert W. Marshall and Ingram Olkin, *Inequalities: Theory of majorization and its applications*, Academic Press, New York, 1979.

[PCR03] S. Sandeep Pradhan, Jim Chou, and Kannan Ramchandran, *Duality between source coding and channel coding and it extension to the side information case*, IEEE Trans. Inform. Theory **49** (2003), no. 5, 1181–1203.

[Sha58] Claude E. Shannon, *Channels with side information at the transmitter*, IBM Journal of Research and Development **2** (1958), 289–293.

[Zam96] Ram Zamir, *The rate loss in the Wyner-Ziv problem*, IEEE Trans. Inform. Theory **42** (1996), no. 6, 2073–2084.

[Zam02] ———, *The half a bit loss of robust source/channel codebooks*, Proc. of the Info. Theory Workshop (Bangalore, India), October 2002, p. 123.

Division of Applied Mathematics, Brown University, Providence, Rhode Island 02912, United States

*E-mail address*: acohen@dam.brown.edu

Research Laboratory for Electronics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, United States

*Current address*: Department of Electrical Engineering, Tel Aviv University, Ramat Aviv 69978, Israel

*E-mail address*: zamir@eng.tau.ac.il