DMT Optimal Code Constructions for Multiuser MIMO Channel

Hsiao-feng Francis Lu and Camilla Hollanti

I. DMT Optimal Codes for General K Users

In the previous work we have proposed a systematic code construction for the multiuser MIMO coded system that is DMT optimal for the case of $K = 2$ users. The code does not require cooperation between the users, and each user encodes his own information by an identical encoder except for a sign change at the second block transmission of the second user. Such sign change, however, complicates the DMT optimal code construction in the general K user case. On the other hand, it is in fact possible to avoid the sign change. In this paper we will present a general systematic construction for K users, $K \geq 2$, that does not require such change and is hence much simpler in encoder implementation.

A. *DMT Optimal Code Constructions for General K and n_t*

Assume that there are K users in the multiuser MIMO system. Each user has a transmitter consisting of n_t antennas and transmits information at multiplexing gain r. Given K, let K_o be the smallest odd integer such that $K_o \geq K$, i.e.

$$K_o = \begin{cases} K+1, & \text{if } K \text{ even,} \\ K, & \text{if } K \text{ odd} \end{cases} \tag{1}$$

Let $\mathbb{K}_o = \mathbb{F}(\eta_o)$ be the number field that is a cyclic Galois extension of $\mathbb{F} = \mathbb{Q}(\imath)$ with degree K_o, and that satisfies $\mathbb{K}_o \cap \mathbb{L} = \mathbb{F}$, where $\mathbb{L} = \mathbb{F}(\theta)$ and $[\mathbb{L} : \mathbb{F}] = n_t$. Let τ_o be the generator of $\mathrm{Gal}(\mathbb{K}_o/\mathbb{F})$ with order K_o, and let $\mathbb{E}_o = \mathbb{K}_o\mathbb{L} = \mathbb{F}(\eta_o, \theta)$. See Fig. 1 for the relation between the required number fields. Let $\mathfrak{D}_o = \left(\mathbb{E}_o/\mathbb{K}_o, \sigma, \zeta = \frac{\gamma}{\gamma^*}\right)$ be a cyclic division algebra,

$$\mathfrak{D}_o = \mathbb{E}_o \oplus z\mathbb{E}_o \oplus \cdots \oplus z^{n_t-1}\mathbb{E}_o, \tag{2}$$

with

$$zx = \sigma(x)z \tag{3}$$

for $x \in \mathfrak{D}_o$, where z is an indeterminate satisfying $z^{n_t} = \zeta \in \mathbb{F}$, and $\gamma \in \mathcal{O}_{\mathbb{F}}$ is some suitable nonnorm element. Notice that $\|\zeta\| = 1$ and that ζ is unimodular. By γ^* we mean the complex conjugate of γ and $\mathcal{O}_{\mathbb{F}}$ is the ring of algebraic integers in field $\mathbb{F}$. It has been shown [1] that with such unimodular ζ, $\mathfrak{D}_o$ is always a cyclic division algebra.

Remark 1: While in the above we have set the nonnorm element ζ to be of form $\zeta = \frac{\gamma}{\gamma^*}$ such that ζ is unimodular, it might be possible in some cases that $\zeta \in \{\pm\imath, -1\}$ is also a legitimate nonnorm and is already unimodular. For such cases, the discussion below can be easily modified and the DMT optimality of the constructions remains to hold. Therefore, for simplicity, here we will focus only on the case of $\zeta = \frac{\gamma}{\gamma^*}$. ■

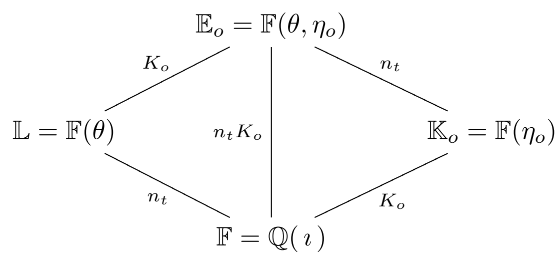

Fig. 1. Field extensions required by the proposed code constructions.

Remark 2: Here we note that by construction the Galois groups of the numbers fields are

$$\begin{aligned} \mathrm{Gal}(\mathbb{E}_o/\mathbb{K}_o) &= \langle\sigma\rangle \\ \mathrm{Gal}(\mathbb{E}_o/\mathbb{L}) &= \langle\tau_o\rangle \\ \mathrm{Gal}(\mathbb{E}_o/\mathbb{F}) &= \langle\tau_o, \sigma\rangle = \langle\tau_o\rangle \times \langle\sigma\rangle \end{aligned}$$

where in the last line the $\langle\tau_o\rangle \times \langle\sigma\rangle$ denotes the direct product of groups generated by τ_o and σ, respectively. ■

Let $\psi_o : \mathfrak{D}_o \to M_{n_t}(\mathbb{E}_o)$ be the left-regular map that maps elements in $\mathfrak{D}_o$ into $n_t \times n_t$ matrices with entries in $\mathbb{E}_o$.

Given multiplexing gain r, let $\mathcal{A}(\mathrm{SNR})$ be the base-alphabet defined as below

$$\mathcal{A}(\mathrm{SNR}) = \left\{ a + b\imath : \begin{array}{r} -\mathrm{SNR}^{\frac{r}{2n_t}} \leq a, b \leq \mathrm{SNR}^{\frac{r}{2n_t}}, \\ a, b \text{ odd} \end{array} \right\}; \tag{4}$$

then the corresponding information set is given by

$$\mathfrak{A}_o(\mathrm{SNR}) = \left\{ \sum_{i=0}^{n_t-1} z^i \sum_{k=0}^{K_o n_t - 1} x_{i,k} e_k : x_{i,k} \in \mathcal{A}(\mathrm{SNR}) \right\}, \tag{5}$$

where $\{e_0, \cdots, e_{K_o n_t - 1}\}$ is an integral basis of $\mathbb{E}_o/\mathbb{F}$.

Having set the above, the information encoding of each user's data stream will proceed as follows. Given the multiplexing gain r, the ith user first divides its binary data steams into blocks of $rK_o \log_2 \mathrm{SNR}$ bits, and then each block of binary bits by using the integral basis $\{e_0, \cdots, e_{K_o n_t - 1}\}$ and the sets $\mathcal{A}(\mathrm{SNR})$ and $\mathfrak{A}_o(\mathrm{SNR})$ defined above can be mapped to some symbol $x_i \in \mathfrak{A}_o(\mathrm{SNR})$ in an one-one fashion. Notice that each user encodes his/her information independently.

Given $x_i \in \mathfrak{A}_o(\mathrm{SNR})$, the information symbol to be transmitted by the ith user, the corresponding $(n_t \times K_o n_t)$ signal matrix S_i that is actually sent out through the user i's transmit antenna array is given by

$$S_i = \kappa \left[\begin{array}{cccc} X_i & \tau_o(X_i) & \cdots & \tau_o^{K_o-1}(X_i) \end{array} \right], \tag{6}$$

where $X_i = \psi_o(x_i)$ and where

$$\kappa^2 \doteq \text{SNR}^{1-\frac{r}{n_t}}$$

is the normalizing constant such that the average signal-to-noise power ratio is SNR. The transmission takes $n_t K_o$ channel uses to complete. It should be noted that in this paper we assume the channel is a Rayleigh block fading channel that is fixed for $n_t K_o$ channel uses. The notations of exponential equality $\doteq$ and inequalities $\dot{\geq}$ and $\dot{\leq}$ are defined in [7].

The overall space-time code for K users is given by

$$\mathcal{S}_o = \left\{ \begin{array}{c} S = \kappa \begin{bmatrix} X_0 & \cdots & \tau_o^{K_o-1}(X_0) \\ \vdots & \ddots & \vdots \\ X_{K-1} & \cdots & \tau_o^{K_o-1}(X_{K-1}) \end{bmatrix} : \\ X_i = \psi(x_i), x_i \in \mathfrak{A}_o(\text{SNR}) \end{array} \right\}, \tag{7}$$

For the purpose of code performance analysis that comes later we set $\mathcal{C}_o = \frac{1}{\kappa}\mathcal{S}_o$, i.e.

$$\mathcal{C}_o = \left\{ \begin{array}{c} C = \begin{bmatrix} X_0 & \cdots & \tau_o^{K_o-1}(X_0) \\ \vdots & \ddots & \vdots \\ X_{K-1} & \cdots & \tau_o^{K_o-1}(X_{K-1}) \end{bmatrix} : \\ X_i = \psi(x_i), x_i \in \mathfrak{A}_o(\text{SNR}) \end{array} \right\}. \tag{8}$$

Given the transmitted information symbol $x_k \in \mathfrak{A}_o(\text{SNR})$ and the channel matrix H_k of the ith user, the jth block received signal matrix at the received end is

$$Y_j = \sum_{k=0}^{K-1} H_k \kappa \tau_o^j(X_k) + W, \quad j = 0, 1, \cdots, K_o - 1, \tag{9}$$

where $X_k = \psi_o(x_k)$ and where W is the noise matrix whose entries are i.i.d. $\mathbb{C}\mathcal{N}(0,1)$ random variables. In other words, we have

$$\begin{bmatrix} Y_0 & \cdots & Y_{K_o-1} \end{bmatrix} = \begin{bmatrix} H_0 & \cdots & H_{K-1} \end{bmatrix} S + W, \tag{10}$$

where $S \in \mathcal{S}_o$ is defined in (7).

To simplify the analysis of the code performance, below we define the extended version of codes $\mathcal{S}_o$ and $\mathcal{C}_o$.

$$\bar{\mathcal{C}}_o = \left\{ \begin{array}{c} \bar{C} = \begin{bmatrix} X_0 & \cdots & \tau_o^{K_o-1}(X_0) \\ \vdots & \ddots & \vdots \\ X_{K_o-1} & \cdots & \tau_o^{K_o-1}(X_{K_o-1}) \end{bmatrix} : \\ X_i = \psi(x_i), x_i \in \mathfrak{A}_o(\text{SNR}) \end{array} \right\}, \tag{11}$$

$$\bar{\mathcal{S}}_o = \left\{ \bar{S} = \kappa \bar{C} \ : \ \bar{C} \in \bar{\mathcal{C}}_o \right\} \tag{12}$$

It is clear that both $\bar{\mathcal{S}}_o$ and $\bar{\mathcal{C}}_o$ are sets of square matrices having size $(K_o n_t \times K_o n_t)$. In particular, we have $\bar{\mathcal{S}}_o = \mathcal{S}_o$ and $\bar{\mathcal{C}}_o = \mathcal{C}_o$ if K odd. Furthermore, given the overall signal matrix $S \in \mathcal{S}_o$, let $\bar{S} \in \bar{\mathcal{S}}_o$ be any signal matrix whose first $K n_t$ rows equals S. Then we can rewrite the received signal matrix given in (10) as

$$\begin{bmatrix} Y_0 & \cdots & Y_{K_o-1} \end{bmatrix} = \begin{bmatrix} H_0 & \cdots & H_{K_o-1} \end{bmatrix} \bar{S} + W, \tag{13}$$

where

$$H_{K_o-1} = \begin{cases} H_{K-1}, & \text{if } K \text{ odd}, \\ \mathbf{0}, & \text{if } K \text{ even}. \end{cases} \tag{14}$$

As (10) and (13) are equivalent, below we will work only with the extended codes $\bar{\mathcal{S}}_o$ and $\bar{\mathcal{C}}_o$, rather than $\mathcal{S}_o$ and $\mathcal{C}_o$.

Lemma 1: For any $\bar{C} \in \bar{\mathcal{C}}_o$

$$\left[(\gamma^*)^{K_o(n_t-1)} \det(\bar{C}) \right] \in \mathbb{Z}[\imath]. \tag{15}$$

Proof: We first claim $\tau_o(\det(\bar{C})) = \det(\bar{C})$. To see this, note that

$$\begin{aligned} &\tau_o(\det(\bar{C})) \\ &= \det \begin{pmatrix} \tau_o(X_0) & \cdots & \tau_o^{K_o}(X_0) \\ \vdots & \ddots & \vdots \\ \tau_o(X_{K_o-1}) & \cdots & \tau_o^{K_o}(X_{K_o-1}) \end{pmatrix} \\ &= \det \begin{pmatrix} \tau_o(X_0) & \cdots & X_0 \\ \vdots & \ddots & \vdots \\ \tau_o(X_{K_o-1}) & \cdots & X_{K_o-1} \end{pmatrix} \\ &= (-1)^{n_t(K_o-1)} \det(\bar{C}) = \det(\bar{C}) \end{aligned}$$

where the last equality follows from the fact $K_o - 1$ is even; hence the claim is proved. Next, we need to show $\sigma(\det(\bar{C})) = \det(\bar{C})$. To this end, define

$$Z = \psi_o(z), \tag{16}$$

where z is the indeterminate of $\mathfrak{D}_o$ defined in (2). By operations in $\mathfrak{D}_o$, it is clear that $\sigma(X) = ZXZ^{-1}$ since $zx = \sigma(x)z$ for $x \in \mathfrak{D}_o$. Now we have

$$\begin{aligned} &\sigma(\det(\bar{C})) \\ &= \begin{vmatrix} ZX_0Z^{-1} & \cdots & \tau_o^{K_o-1}(ZX_0Z^{-1}) \\ \vdots & \ddots & \vdots \\ ZX_{K_o-1}Z^{-1} & \cdots & \tau_o^{K_o-1}(ZX_{K_o-1}Z^{-1}) \end{vmatrix} \\ &= \begin{vmatrix} ZX_0Z^{-1} & \cdots & Z\tau_o^{K_o-1}(X_0)Z^{-1} \\ \vdots & \ddots & \vdots \\ ZX_{K_o-1}Z^{-1} & \cdots & Z\tau_o^{K_o-1}(X_{K_o-1})Z^{-1} \end{vmatrix} \\ &= \begin{vmatrix} Z & & \\ & \ddots & \\ & & Z \end{vmatrix} \times \\ &\quad \begin{vmatrix} X_0 & \cdots & \tau_o^{K_o-1}(X_0) \\ \vdots & \ddots & \vdots \\ X_{K_o-1} & \cdots & \tau_o^{K_o-1}(X_{K_o-1}) \end{vmatrix} \begin{vmatrix} Z^{-1} & & \\ & \ddots & \\ & & Z^{-1} \end{vmatrix} \\ &= \det(\bar{C}) \end{aligned}$$

where we have used the fact that $\tau_o(Z) = Z$ since $0 \neq \zeta \in \mathbb{F}$ by construction. Thus, as $\det(\bar{C})$ is fixed by both τ_o and σ, we see $\det(\bar{C}) \in \mathbb{Q}(\imath)$.

Finally note that the matrix

$$\tau_o^j(X_i)\begin{bmatrix} 1 & & & \\ & \gamma^* & & \\ & & \ddots & \\ & & & \gamma^* \end{bmatrix}$$

has entries in $\mathcal{O}_{\mathbb{E}_o}$ for all $i = 0, 1, \cdots, K_o - 1$ and $j = 0, 1, \cdots, n_t - 1$, hence we have

$$\left[(\gamma^*)^{K_o(n_t-1)} \det(\bar{C})\right] \in \mathcal{O}_{\mathbb{E}_o}.$$

$\mathcal{O}_{\mathbb{E}_o}$ is the ring of algebraic integers in number field $\mathbb{E}_o$.

Therefore, we conclude that

$$\left[(\gamma^*)^{K_o(n_t-1)} \det(\bar{C})\right] \in \mathcal{O}_{\mathbb{E}_o} \cap \mathbb{Q}(\imath) = \mathbb{Z}[\imath]$$

and this completes the proof. ■

Lemma 2: Let

$$\mathfrak{C} = \begin{bmatrix} \underline{c}_0^t \\ \vdots \\ \underline{c}_{K_o-1}^t \end{bmatrix} = \begin{bmatrix} x_0 & \cdots & \tau_o^{K_o-1}(x_0) \\ \vdots & \ddots & \vdots \\ x_{K_o-1} & \cdots & \tau_o^{K_o-1}(x_{K_o-1}) \end{bmatrix}$$

and

$$\bar{C} = \begin{bmatrix} X_0 & \cdots & \tau_o^{K_o-1}(X_0) \\ \vdots & \ddots & \vdots \\ X_{K_o-1} & \cdots & \tau_o^{K_o-1}(X_{K_o-1}) \end{bmatrix}$$

with $X_i = \psi_o(x_i)$. Let m be the maximal number such that the set $\{\underline{c}_{i_1}^t, \cdots, \underline{c}_{i_m}^t\}$ is linearly independent as a left $\mathfrak{D}_o$ module, where $\{i_1, \cdots, i_m\} \subseteq \{0, 1, \cdots, K_o - 1\}$; then

$$\text{rank}(\bar{C}) \;=\; mn_t \tag{17}$$

where the rank is measured in $\mathbb{C}$.

Proof: To find out the rank of the matrix $\bar{C}$, we follow Gaussian elimination method using elementary row operations. In particular, it should be noted that the same row operations can be carried out in $\mathfrak{C}$ whose entries are in the cyclic division algebra $\mathfrak{D}_o$, with some extra care as the multiplications in $\mathfrak{D}_o$ are non-commutative. Further, we note that elementary row operations on $\mathfrak{C}$ are equivalent to the block elementary row operations on $\bar{C}$. Specifically, say P is an $(K_o \times K_o)$ elementary matrix with entries in $\mathfrak{D}_o$; then it is clear that

$$\Psi_o(P\mathfrak{C}) \;=\; \Psi_o(P)\bar{C},$$

where Ψ_o is the natural extension of ψ_o to the $(K_o \times K_o)$ matrix algebra $M_{K_o}(\mathfrak{D}_o)$ over $\mathfrak{D}_o$, i.e.

$$\Psi_o(P) = \left[\psi_o(P_{i,j})\right]. \tag{18}$$

Now it follows from hypothesis that $\{\underline{c}_{i_1}^t, \cdots, \underline{c}_{i_m}^t\}$ is the maximal subset of the rows of $\mathfrak{C}$ that are linearly independent over $\mathfrak{D}_o$; there are m leading ones in the row-reduced matrix of $\mathfrak{C}$. Equivalently, this reduces the matrix $\bar{C}$ into a matrix whose main diagonal consists of m identity matrices of size $(n_t \times n_t)$, after permuting the columns. This completes the proof. ■

The above lemma shows that the overall code matrix $\bar{C} \in \mathcal{C}_o$ does not always have full rank $K_o n_t$, and when that happens the resulting rank is always a multiple of n_t. On the other hand, when $\bar{C}$ is singular, $\det(\bar{C}) = 0$ and we can show a weaker version of Lemma 1.

Lemma 3: Let $\mathfrak{C}$ be defined as in Lemma 2 and assume that $\{\underline{x}_{i_1}^t, \cdots, \underline{x}_{i_m}^t\}$ is the maximal subset of rows of $\mathfrak{C}$ that are linearly independent as a left $\mathfrak{D}_o$ module. Define

$$\mathfrak{C}_s = \begin{bmatrix} \underline{x}_{i_1}^t \\ \vdots \\ \underline{x}_{i_m}^t \end{bmatrix} \quad \text{and } \bar{C}_s = \Psi_o(\mathfrak{C}_s) \tag{19}$$

i.e. $\bar{C}_s$ is the submatrix of $\bar{C}$ consisting of mn_t rows, where $\Psi_o(\cdot)$ is defined in (18). Then

$$1 < \left[\|\gamma\|^{2mn_t} \cdot \det\left(\bar{C}_s\bar{C}_s^\dagger\right)\right] \in \mathbb{Z}. \tag{20}$$

Proof: The part of $0 < \left[\|\gamma\|^{2mn_t} \cdot \det\left(\bar{C}_s\bar{C}_s^\dagger\right)\right]$ follows from Lemma 2 since the matrix $\bar{C}_s$ has full row rank mn_t. Next we will verify that $\det\left(\bar{C}_s\bar{C}_s^\dagger\right)$ is fixed under the automorphisms τ_o and σ. For τ_o, it can be seen from the proof of Lemma 1 that

$$\tau_o\left(\det\left(\bar{C}_s\bar{C}_s^\dagger\right)\right) = \det\left(\tau_o\left(\bar{C}_s\right)\left[\tau_0\left(\bar{C}_s\right)\right]^\dagger\right)$$

and

$$\begin{aligned} &\tau_o(\bar{C}_s) \\ &= \det\begin{pmatrix} \tau_o(X_{i_1}) & \cdots & \tau_o^{K_o}(X_{i_1}) \\ \vdots & \ddots & \vdots \\ \tau_o(X_{i_m-1}) & \cdots & \tau_o^{K_o}(X_{i_m-1}) \end{pmatrix} \\ &= \bar{C}_s P \end{aligned}$$

for some column permutation matrix P of size $(K_o n_t \times K_o n_t)$. Now it follows that

$$\det\left(\tau_o\left(\bar{C}_s\right)\tau_0\left(\bar{C}_s\right)^\dagger\right) = \det\left(\bar{C}_s P P^\dagger \bar{C}_s^\dagger\right) = \det\left(\bar{C}_s\bar{C}_s^\dagger\right)$$

as $PP^\dagger = I_{K_o n_t}$, and we have proved $\det\left(\bar{C}_s\bar{C}_s^\dagger\right)$ is fixed under τ_o.

For σ, again recall from the proof of Lemma 1 that

$$\sigma\left(\det\left(\bar{C}_s\bar{C}_s^\dagger\right)\right) = \det\left(\sigma\left(\bar{C}_s\right)\left[\sigma\left(\bar{C}_s\right)\right]^\dagger\right)$$

and that

$$\begin{aligned} &\sigma(\bar{C}_s) \\ &= \begin{bmatrix} ZX_{i_1}Z^{-1} & \cdots & Z\tau_o^{K_o-1}(X_{i_1})Z^{-1} \\ \vdots & \ddots & \vdots \\ ZX_{i_m}Z^{-1} & \cdots & Z\tau_o^{K_o-1}(X_{i_m})Z^{-1} \end{bmatrix} \\ &= \begin{bmatrix} Z & & \\ & \ddots & \\ & & Z \end{bmatrix} \bar{C}_s \begin{bmatrix} Z^{-1} & & \\ & \ddots & \\ & & Z^{-1} \end{bmatrix}, \end{aligned}$$

where

$$Z = \psi_o(z) = \begin{bmatrix} 0 & 0 & 0 & \cdots & \zeta \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix}. \tag{21}$$

From the above it is clear that $ZZ^\dagger = I_{n_t}$ since $\zeta\zeta^* = 1$ by construction, and $Z^{-1}\left(Z^{-1}\right)^\dagger = I_{n_t}$. Thus, we see

$$\sigma(\bar{C}_s)\left[\sigma(\bar{C}_s)\right]^\dagger = \mathrm{diag}(Z,\cdots,Z)\,\bar{C}_s\,\bar{C}_s^\dagger\,\mathrm{diag}(Z^\dagger,\cdots,Z^\dagger)$$

and hence $\sigma\det(\bar{C}_s\bar{C}_s^\dagger) = \det(\bar{C}_s\bar{C}_s^\dagger)$. So far, we have proved that $\det(\bar{C}_s\bar{C}_s^\dagger)$ is fixed by both τ_o and σ, and this means that $\det(\bar{C}_s\bar{C}_s^\dagger) \in \mathbb{Q}\cap\mathbb{R} = \mathbb{Q}$. Finally, the proof is complete after noting that $\gamma^*\bar{C}_s$ has entries in $\mathcal{O}_{\mathbb{E}_o}$. ∎

Theorem 4: Given the multiplexing gain r, the proposed code $\mathcal{S}_o$ defined in (7) achieves the DMT

$$d(r) = \min_{1\le k\le K} d^*_{kn_t,n_r}(kr) \tag{22}$$

over quasi-static Rayleigh fading channel with coherence time $T \ge K_o n_t$. Thus, $\mathcal{S}_o$ is DMT optimal.

Proof: The proof is relegated to Section II. ∎

II. Proof of Theorem 4

Here we only prove the case of K odd, and the case of K even can be proved by a similar argument. We will discuss the case of even K in a remark following the proof.

For any $\bar{C} \neq \bar{C}' \in \bar{\mathcal{C}}_o$ with

$$\bar{C} = \begin{bmatrix} \psi_o(x_0) & \cdots & \tau_o^{K_o-1}\left(\psi_o(x_0)\right) \\ \vdots & \ddots & \vdots \\ \psi_o(x_{K_o-1}) & \cdots & \tau_o^{K_o-1}\left(\psi_o(x_{K_o-1})\right) \end{bmatrix}$$

and

$$\bar{C}' = \begin{bmatrix} \psi_o(x_0') & \cdots & \tau_o^{K_o-1}\left(\psi_o(x_0')\right) \\ \vdots & \ddots & \vdots \\ \psi_o(x_{K_o-1}') & \cdots & \tau_o^{K_o-1}\left(\psi_o(x_{K_o-1}')\right) \end{bmatrix}$$

let $\bar{S} = \kappa\bar{C}$, $\bar{S}' = \kappa\bar{C}'$, and let $H = [H_0\cdots H_{K_o-1}]$, where H_i is the $(n_r\times n_t)$ channel matrix associated with the ith user.

A. Lower Bounds on the Minimum Distances of Received Signal Matrices

Given the channel matrix H, below we provide a lower bound on the squared Euclidean distance between $H\bar{S}$ and $H\bar{S}'$, i.e.

$$d_E^2\left(\bar{S},\bar{S}'\right) = \Bigg\| H\underbrace{\left(\bar{S}-\bar{S}'\right)}_{:=\Delta\bar{S}} \Bigg\|_F^2 \tag{23}$$

where by $\|A\|_F$ we mean the Frobenius (or ℓ^2-) norm of matrix A. We distinguish the following two cases.

1) $x_\ell \neq x_\ell'$ for $\ell \in \{i_1,\cdots,i_m\}$ and $x_\ell = x_\ell'$ otherwise. Further we assume $\mathrm{rank}(\bar{C}-\bar{C}') = mn_t$: In other words, here we consider the case when out of K_o x_ℓ's, m of them are distinct and the m rows $\left[(x_\ell - x_\ell')\cdots\tau_o^{K_o-1}\left(x_\ell - x_\ell'\right)\right]$ formed by such x_ℓ's are all linearly independent as a left $\mathfrak{D}_o$ module over $\mathfrak{D}_o$.
In this case, let $\bar{C}_s$ and $\bar{C}_s'$ be defined as in (19) and let

$$H_s = [H_{i_1}\cdots H_{i_m}]$$

be the equivalent $(n_r\times mn_t)$ channel matrix; then we have

$$d_E^2(\bar{S},\bar{S}') = \left\|\kappa H_s\left(\bar{C}_s - \bar{C}_s'\right)\right\|_F^2$$

Let $\lambda_{1,1}^{(m)} \le \cdots \le \lambda_{1,Q_m}^{(m)}$ be the set of ordered nonzero eigenvalues of $H_sH_s^\dagger$ where $Q_m = \min\{mn_t, n_r\}$ and let $\ell_{1,1} \ge \cdots \ge \ell_{1,mn_t} > 0$ be the ordered nonzero eigenvalues of $\left(\bar{C}_s - \bar{C}_s'\right)\left(\bar{C}_s-\bar{C}_s'\right)^\dagger$. Then we have

$$d_E^2(\bar{S},\bar{S}') \ \ge\ \kappa^2\sum_{i=1}^{Q_m}\lambda_{1,i}^{(m)}\ell_{1,mn_t-Q_m+i}, \tag{24}$$

where it should be noted that

$$\prod_{i=1}^{mn_t}\ell_{1,i} \ge \frac{1}{\|\gamma\|^{2mn_t}} \ \doteq\ 1. \tag{25}$$

The first inequality follows from Lemma 3 and the second exponential equality is because γ is fixed and is independent of SNR.

By repeatedly using the arithmetic mean-geometric mean inequality and (25) as in [2], [3] given k, $k = 1,2,\cdots,Q_m$, we have

$$\begin{aligned}
& d_E^2(\bar{S},\bar{S}') \qquad (26)\\
\ge\ & \kappa^2\sum_{i=Q_m-k+1}^{Q_m}\lambda_{1,i}^{(m)}\ell_{1,mn_t-Q_m+i} \\
\dot{\ge}\ & \kappa^2\left[\prod_{i=Q_m-k+1}^{Q_m}\lambda_{1,i}^{(m)}\right]^{\frac{1}{k}}\times \\
& \left[\prod_{i=Q_m-k+1}^{Q_m}\ell_{1,mn_t-Q_m+i}\right]^{\frac{1}{k}} \\
\dot{\ge}\ & \kappa^2\left[\prod_{i=Q_m-k+1}^{Q_m}\lambda_{1,i}^{(m)}\right]^{\frac{1}{k}}\left[\prod_{i=1}^{mn_t-k}\ell_{1,i}\right]^{-\frac{1}{k}} \qquad (27)\\
\dot{\ge}\ & \kappa^2\left[\prod_{i=Q_m-k+1}^{Q_m}\lambda_{1,i}^{(m)}\right]^{\frac{1}{k}}\left[\sum_{i=1}^{mn_t-k}\ell_{1,i}\right]^{-\frac{mn_t-k}{k}} \\
\dot{\ge}\ & \kappa^2\left[\prod_{i=Q_m-k+1}^{Q_m}\lambda_{1,i}^{(m)}\right]^{\frac{1}{k}}\left\|\bar{C}_s-\bar{C}_s'\right\|_F^{-\frac{mn_t-k}{k}} \\
\dot{\ge}\ & \mathrm{SNR}^{1-\frac{r}{n_t}}\left[\prod_{i=Q_m-k+1}^{Q_m}\lambda_{1,i}^{(m)}\right]^{\frac{1}{k}}\mathrm{SNR}^{-\frac{r}{n_t}\frac{mn_t-k}{k}} \\
:=\ & \mathrm{SNR}^{\delta_{1,k}^{(m)}(\underline{\alpha}_1^{(m)})} \qquad (28)
\end{aligned}$$

where (27) follows from (25) and where in (28) we have set

$$\begin{aligned}
\lambda_{1,i}^{(m)} &= \mathrm{SNR}^{-\alpha_{1,i}^{(m)}}, \\
\underline{\alpha}_1^{(m)} &= \left[\alpha_{1,1}^{(m)}\cdots\alpha_{1,Q_m}^{(m)}\right]^t
\end{aligned}$$

Hence

$$\delta_{1,k}^{(m)}(\underline{\alpha}_1^{(m)}) := \frac{1}{k}\left[\sum_{i=Q_m-k+1}^{Q_m}\left(1-\alpha_{1,i}^{(m)}\right)\right] - \frac{rm}{k}. \tag{29}$$

2) The second case is when $x_\ell \neq x'_\ell$ for $\ell \in \{i_1, \cdots, i_m\}$ and $x_i = x'_i$ otherwise. But $\operatorname{rank}\left(\bar{C}-\bar{C}'\right) < mn_t$: In other words, the m nonzero rows formed by $\left[(x_\ell - x'_\ell) \cdots \tau_o^{K_o-1}(x_\ell - x'_\ell)\right]$ are not linearly independent over $\mathfrak{D}_o$. From Lemma 2 we can assume without loss of generality that $\operatorname{rank}\left(\bar{C}-\bar{C}'\right) = nn_t$ and that

$$\left\{\left[(x_\ell - x'_\ell) \cdots \tau_o^{K_o-1}(x_\ell - x'_\ell)\right] : \ell = i_1, \cdots, i_n\right\}$$

are linearly independent for some $n < m$. Clearly $n > 1$ since ψ_o is an injection.
Now let $dx_\ell := x_\ell - x'_\ell$ and let $\bar{C}_s$ and $\bar{C}'_s$ be defined as (19) of Lemma 3 with respect to the set $\{i_1, \cdots, i_m\}$. Set $\Delta\bar{C}_s = \bar{C}_s - \bar{C}'_s$ and $\Delta X_\ell = \psi_o(x_\ell - x'_\ell)$. Lemma 2 in turn implies that

$$\Delta\bar{C}_s = \begin{bmatrix} I_{n_t} & & \\ & \ddots & \\ & & I_{n_t} \\ P_{i_{n+1},1} & \cdots & P_{i_{n+1},n} \\ \vdots & \vdots & \vdots \\ P_{i_m,1} & \cdots & P_{i_m,n} \end{bmatrix} \mathbf{\Delta X} \tag{30}$$

where

$$\mathbf{\Delta X} := \begin{bmatrix} \Delta X_{i_1} & \cdots & \tau_o^{K_o-1}\left(\Delta X_{i_1}\right) \\ \vdots & \ddots & \vdots \\ \Delta X_{i_n} & \cdots & \tau_o^{K_o-1}\left(\Delta X_{i_n}\right) \end{bmatrix} \tag{31}$$

Let

$$H_s = \begin{bmatrix} H_{i_1} & \cdots & H_{i_m} \end{bmatrix}$$

be the equivalent channel matrix; then the difference of the noise-free received signal matrices is given by

$$\kappa H_s \Delta\bar{C}_s = \kappa \mathbf{H}_{eq}\,\mathbf{\Delta X} \tag{32}$$

where $\mathbf{H}_{eq} = \left[\tilde{H}_1 \cdots \tilde{H}_n\right]$ is an alternative channel equivalent matrix and

$$\tilde{H}_\ell := H_{i_\ell} + \sum_{k=n+1}^{m} H_{i_k} P_{i_k,\ell} \tag{33}$$

for $\ell = 1, \cdots, n$.
Let $\lambda_{2,1}^{(m,n)} \leq \cdots \leq \lambda_{2,Q_n}^{(m,n)}$ be the set of ordered nonzero eigenvalues of $\mathbf{H}_{eq}\mathbf{H}_{eq}^\dagger$ where $Q_n = \min\{nn_t, n_r\}$ and let $\ell_{2,1} \geq \cdots \geq \ell_{2,nn_t} > 0$ be the ordered nonzero eigenvalues of $\mathbf{\Delta X \Delta X}^\dagger$. Notice that

$$\prod_{i=1}^{nn_t} \ell_{2,i} = \det\left(\mathbf{\Delta X \Delta X}^\dagger\right) \geq \frac{1}{\|\gamma\|^{2nn_t}} \doteq 1$$

from Lemma 3. Arguing similarly as the first case shows that

$$d_E^2(\bar{S}, \bar{S}') \geq \mathsf{SNR}^{\delta_{2,k}^{(m,n)}(\underline{\alpha}_2^{(m,n)})} \tag{34}$$

where

$$\lambda_{2,i}^{(m,n)} := \mathsf{SNR}^{-\alpha_{2,i}^{(m,n)}}, \tag{35}$$

$$\underline{\alpha}_2^{(m,n)} = \left[\alpha_{2,1}^{(m,n)} \cdots \alpha_{2,Q_n}^{(m,n)}\right]^t, \tag{36}$$

and

$$\delta_{2,k}^{(m,n)}(\underline{\alpha}_2^{(m,n)}) := \frac{1}{k}\left[\sum_{i=Q_n-k+1}^{Q_n}\left(1-\alpha_{2,i}^{(m,n)}\right)\right] - \frac{rn}{k}. \tag{37}$$

Summarizing from the above we obtain a general lower bound on $d_E^2(\bar{S}, \bar{S}')$,

$$\begin{aligned} & d_E^2(\bar{S}, \bar{S}') \\ \geq\ & \min_{\bar{S}\neq\bar{S}'} d_E^2(\bar{S}, \bar{S}') \\ \geq\ & \min\left\{\min_m \max_k \mathsf{SNR}^{\delta_{1,k}^{(m)}(\underline{\alpha}_1^{(m)})},\right. \\ & \left.\min_{m,n} \max_k \mathsf{SNR}^{\delta_{2,k}^{(m,n)}(\underline{\alpha}_2^{(m,n)})}\right\} \\ :=\ & d_{E,\min}^2 := \mathsf{SNR}^{\delta_{\min}}. \end{aligned} \tag{38}$$

It should be noted that $d_{E,\min}^2$ is a random variable, and is a function of the random matrix $H = [H_0, \cdots, H_{K_o-1}]$. Furthermore, $d_{E,\min}^2$ plays the role of minimum Euclidean distance among all noise-free received signal matrices. In other words, it resembles the minimum Hamming distance in conventional nonlinear error correcting codes over finite fields.

B. Upper Bounds of Codeword Error Probability

Having obtained the squared minimum Euclidean distance $d_{E,\min}^2$ among all possible noise-free received signal matrices, below we proceed to analyze the error performance of the proposed construction. The analysis makes use of the sphere bounding technique proposed in [2], [3]. The codeword error probability at multiplexing gain r given channel matrix H can be upper bounded by

$$\begin{aligned} & P_{\text{cwe}}\left(r|H\right) \\ \leq\ & \Pr\left\{\|W\|_F^2 \geq \frac{d_{E,\min}^2}{4}\right\} \\ =\ & \exp\left(-\frac{d_{E,\min}^2}{4}\right)\sum_{j=0}^{K_o n_r n_t-1}\frac{(d_{E,\min}^2)^j}{j!}, \end{aligned} \tag{39}$$

and it should be noted that the RHS $\doteq 0$ if $\delta_{\min} > 0$. Since $P_{\text{cwe}}\left(r|H\right) \leq 1$, it follows that

$$\begin{aligned} & P_{\text{cwe}}(r) = \mathbb{E}_H P_{\text{cwe}}\left(r|H\right) \\ & \leq \Pr\left\{H : \delta_{\min} \leq 0\right\} \\ & \leq \sum_{m=1}^{K_o}\binom{K_o}{m}\Pr\left\{H : \max_k \delta_{1,k}^{(m)}(\underline{\alpha}_1^{(m)}) \leq 0\right\} + \\ & \sum_{m=1}^{K_o}\binom{K_o}{m}\sum_{n=1}^{m-1}\binom{m}{n}\Pr\left\{H : \max_k \delta_{2,k}^{(m,n)}(\underline{\alpha}_2^{(m,n)}) \leq 0\right\} \end{aligned} \tag{40}$$

where the last inequality follows from the union bound of probabilistic events. Further, in (40) we have over-counted in the second summand the number of choices of n $\mathfrak{D}_o$-linearly independent rows out of m nonzero rows in the different matrix $[\tau_o^j(x_i - x_i')]_{i=0}^{K_o-1}{}_{j=0}^{K_o-1}$. Yet, even with this over-estimate, as

$$\binom{K_o}{m}, \binom{m}{n} \doteq 1$$

for all m, n within the designated range, we can rewrite (40) as

$$\begin{aligned} P_{\text{cwe}}(r) \quad \dot{\leq} \quad & \max\Bigg\{\max_m \Pr\left\{H : \max_k \delta_{1,k}^{(m)}(\underline{\alpha}_1^{(m)}) \leq 0\right\} \\ & \max_{m,n} \Pr\left\{H : \max_k \delta_{2,k}^{(m,n)}(\underline{\alpha}_2^{(m,n)}) \leq 0\right\}\Bigg\} \end{aligned} \quad (41)$$

Below we investigate the diversity order of each term in (41).

C. Diversity Gain of the First Case

For each m, $1 \leq m \leq K_0$, we have

$$\begin{aligned} & \Pr\left\{H : \max_k \delta_{1,k}^{(m)}(\underline{\alpha}_1^{(m)}) \leq 0\right\} \\ = \;& \Pr\left\{H : \begin{array}{l} \frac{1}{k}\left[\sum_{i=Q_m-k+1}^{Q_m}\left(1-\alpha_{1,i}^{(m)}\right)\right] - \frac{rm}{k} \leq 0, \\ \text{all } k, \text{ and } \alpha_{1,1}^{(m)} \geq \alpha_{1,2}^{(m)} \cdots \geq \alpha_{1,Q_m}^{(m)} \end{array}\right\} \\ = \;& \Pr\left\{H : \sum_{i=1}^{Q_m}\left(1-\alpha_{1,i}^{(m)}\right)^+ \leq rm\right\} \quad (42) \\ = \;& \Pr\left\{H : \log\det\left(I_{n_r} + \text{SNR} H_s H_s^\dagger\right) \leq rm \log \text{SNR}\right\} \quad (43) \\ \doteq \;& \text{SNR}^{-d^*_{mn_t,n_r}(rm)} \quad (44) \end{aligned}$$

where $Q_m := \min\{mn_t, n_r\}$ and where in (43) $H_s := [H_{i_1} \cdots H_{i_m}]$. (42) follows from [4]–[6] where $(x)^+ = \max\{x, 0\}$ for $x \in \mathbb{R}$. (44) is given in [7] since H_s is of size $(n_r \times mn_t)$.

Furthermore, in (44) $d^*_{p,q}(s)$ represents the optimal diversity gain tradeoff of a $(p \times q)$ MIMO Rayleigh fading channel at multiplexing gain s and is given by a piecewise linear function connecting the points $(s, (p-s)(q-s))$ for $s = 0, 1, \cdots, \min\{p, q\}$.

D. Diversity Gain of the Second Case

Similarly, for the second kind of maximizations in (41) we have for each $1 \leq n < m \leq K_o$ that

$$\begin{aligned} & \Pr\left\{H : \max_k \delta_{2,k}^{(m,n)}(\underline{\alpha}_2^{(m,n)}) \leq 0\right\} \\ & = \Pr\left\{H : \begin{array}{l} \frac{1}{k}\left[\sum_{i=Q_n-k+1}^{Q_n}\left(1-\alpha_{2,i}^{(m,n)}\right)\right] - \frac{rn}{k} \leq 0, \\ \text{all } k, \text{ and } \alpha_{2,1}^{(m,n)} \geq \alpha_{2,2}^{(m,n)} \cdots \geq \alpha_{2,Q_n}^{(m,n)} \end{array}\right\} \\ & = \Pr\left\{H : \sum_{i=1}^{Q_n}\left(1-\alpha_{2,i}^{(m,n)}\right)^+ \leq rn\right\} \\ & = \Pr\left\{H : \log\det\left(I_{n_r} + \text{SNR}\mathbf{H}_{eq}\mathbf{H}_{eq}^\dagger\right) \leq rn \log\text{SNR}\right\} \quad (45) \end{aligned}$$

where

$$\begin{aligned} \mathbf{H}_{eq} &= \left[\begin{array}{ccc} \tilde{H}_1 & \cdots & \tilde{H}_n \end{array}\right] \\ &= \left[\begin{array}{ccc} H_{i_1} & \cdots & H_{i_m} \end{array}\right] \left[\begin{array}{ccc} I_{n_t} & & \\ & \ddots & \\ & & I_{n_t} \\ P_{i_{n+1},1} & \cdots & P_{i_{n+1},n} \\ \vdots & \vdots & \vdots \\ P_{i_m,1} & \cdots & P_{i_m,n} \end{array}\right] \end{aligned} \quad (46)$$

that is, $\tilde{H}_\ell = H_{i_\ell} + \sum_{k=n+1}^m H_{i_k} P_{i_k,\ell}$ for $\ell = 1, \cdots, n$. The matrices $P_{i,j}$ are defined in (30).

To analyze the probability of (45), set

$$\mathbf{H}_{s,1} := \left[\begin{array}{ccc} H_{i_1} & \cdots & H_{i_n} \end{array}\right] \quad (47)$$

$$\mathbf{H}_{s,2} = \left[\begin{array}{ccc} H_{i_{n+1}} & \cdots & H_{i_m} \end{array}\right] \quad (48)$$

$$\mathbf{P}_{m,n} = \left[\begin{array}{ccc} P_{i_{n+1},1} & \cdots & P_{i_{n+1},n} \\ \vdots & \vdots & \vdots \\ P_{i_m,1} & \cdots & P_{i_m,n} \end{array}\right], \quad (49)$$

and we can rewrite (46) as

$$\mathbf{H}_{eq} = \mathbf{H}_{s,1} + \mathbf{H}_{s,2}\mathbf{P}_{m,n}. \quad (50)$$

$\mathbf{H}_{s,1}$ is of size $(n_r \times nn_t)$, $\mathbf{H}_{s,2}$ is of size $(n_r \times (m-n)n_t)$, and $\mathbf{P}_{m,n}$ is of size $((m-n)n_t \times nn_t)$.

Let $(\underline{h}_{eq,i})^t$ denote the ith row of matrix $\mathbf{H}_{eq}$, $i = 1, 2, \cdots, n_r$; then since the entries of matrices $\mathbf{H}_{s,1}$ and $\mathbf{H}_{s,2}$ are i.i.d. $\mathbb{C}\mathcal{N}(0,1)$ random variables, the covariance matrix of $\underline{h}_{eq,i}^t$ is

$$\mathbf{\Sigma} = \mathbb{E}(\underline{h}_{eq,i})(\underline{h}_{eq,i})^\dagger = I_{nn_t} + \mathbf{P}_{m,n}^t\mathbf{P}_{m,n}^*. \quad (51)$$

$(\underline{h}_{eq,i})^t$ and $(\underline{h}_{eq,j})^t$ are statistically independent for all $i \neq j$ and

$$\mathbb{E}(\underline{h}_{eq,i})(\underline{h}_{eq,j})^\dagger = \mathbf{0}.$$

Since $\mathbf{\Sigma}$ is hermitian symmetric positive definite, by spectrum theorem of hermitian symmetric nonnegative definite matrices we have

$$\mathbf{\Sigma} = \mathbf{U}^t\mathbf{\Xi}\mathbf{U}^* = \mathbf{U}^t\left(I_{nn_t} + \mathbf{\Lambda}\right)\mathbf{U}^* \quad (52)$$

where $\mathbf{U}^t\mathbf{\Lambda}\mathbf{U}^*$ is the eigen-decomposition of $\mathbf{P}_{m,n}^t\mathbf{P}_{m,n}^*$. $\mathbf{\Xi} = I_{nn_t} + \mathbf{\Lambda}$ is an $(nn_t \times nn_t)$ diagonal matrix whose diagonal values are the eigenvalues of $\mathbf{\Sigma}$. Moreover, these eigenvalues are lower bounded by 1. $\mathbf{U}$ is an $(nn_t \times nn_t)$ unitary matrix consisting of unit-norm eigenvectors of $\mathbf{\Sigma}$.

Since entries of $\mathbf{H}_{eq}$ are jointly complex Gaussian, we can apply simulation theorem to simulate $\mathbf{H}_{eq}$. To this end, let G be an $(n_r \times nn_t)$ matrix whose entries are i.i.d. $\mathbb{C}\mathcal{N}(0,1)$ random variables and set

$$G_s = G\sqrt{\mathbf{\Xi}}\,\mathbf{U}. \quad (53)$$

By Karhunen-Loève expansion, G_s is statistically equivalent to the matrix $\mathbf{H}_{eq}$, meaning that G_s and $\mathbf{H}_{eq}$ have the same joint probabilistic density functions.

As a short summary, the above analysis shows

$$\begin{aligned}&\Pr\left\{H:\log\det\left(I_{n_r}+\mathrm{SNR}\mathbf{H}_{eq}\mathbf{H}_{eq}^{\dagger}\right)\le rn\log\mathrm{SNR}\right\}\\ =\;&\Pr\left\{G_s:\log\det\left(I_{n_r}+\mathrm{SNR}G_sG_s^{\dagger}\right)\le rn\log\mathrm{SNR}\right\}\\ =\;&\Pr\left\{G:\log\det\left(I_{n_r}+\mathrm{SNR}G\Xi G^{\dagger}\right)\le rn\log\mathrm{SNR}\right\}\end{aligned}\tag{54}$$

Next, we will use Minkowski determinant inequality [8] for positive definite matrices to study the probability given in (54). The Minkowski determinant inequality states

$$\left[\det\left(A+B\right)\right]^{1/n}\;\ge\;\left[\det\left(A\right)\right]^{1/n}+\left[\det\left(B\right)\right]^{1/n},\tag{55}$$

if A and B are $(n\times n)$ positive definite matrices. Thus, for some very small ϵ, $0<\epsilon<1$ we set

$$\begin{aligned}A&=(1-\epsilon)I_{n_r}+\mathrm{SNR}GG^{\dagger}\\ B&=\epsilon I_{n_r}+\mathrm{SNR}G\mathbf{\Lambda}G^{\dagger}\end{aligned}$$

where it should be noted that B is a positive definite matrix with probability one (W.P.1). The Minkowski determinant inequality then shows that

$$\begin{aligned}&\left[\det\left(I_{n_r}+\mathrm{SNR}G\Xi G^{\dagger}\right)\right]^{1/n_r}\\ =\;&\left[\det\left(A+B\right)\right]^{1/n_r}\\ \ge\;&\left[\det\left(A\right)\right]^{1/n_r}+\left[\det\left(B\right)\right]^{1/n_r}\qquad\text{(W.P.1)}\\ \ge\;&\left[\det\left(A\right)\right]^{1/n_r}\\ \doteq\;&\left[\det\left(I_{n_r}+\mathrm{SNR}GG^{\dagger}\right)\right]^{1/n_r},\end{aligned}$$

where the last exponential equality follows from $(1-\epsilon)\doteq\mathrm{SNR}^0$ when $\epsilon\to 0$. Hence

$$\log\det\left(I_{n_r}+\mathrm{SNR}G\Xi G^{\dagger}\right)\;\dot{\ge}\;\log\det\left(I_{n_r}+\mathrm{SNR}GG^{\dagger}\right)\tag{56}$$

with probability one. It in turn implies

$$\begin{aligned}&\Pr\left\{\log\det\left(I_{n_r}+\mathrm{SNR}G\Xi G^{\dagger}\right)\le rn\log\mathrm{SNR}\right\}\\ \dot{\le}\;&\Pr\left\{\log\det\left(I_{n_r}+\mathrm{SNR}GG^{\dagger}\right)\le rn\log\mathrm{SNR}\right\}\\ \doteq\;&\mathrm{SNR}^{-d^*_{nn_t,n_r}(nr)}.\end{aligned}\tag{57}$$

Summarizing results of (41), (44) and (57) gives

$$P_{\text{cwe}}(r)\;\dot{\le}\;\mathrm{SNR}^{-d(r)}\tag{58}$$

and

$$\begin{aligned}d(r)\;&:=\;\min_{n<m}\left\{d^*_{mn_t,n_r}(mr),d^*_{nn_t,n_r}(nr)\right\}&(59)\\ &=\;\min_{m}\left\{d^*_{mn_t,n_r}(mr)\right\}.&(60)\end{aligned}$$

This proves the DMT optimality of the construction.

E. Proof Outline for K Even

For the case when the number of users K is even, the proof of Theorem 4 can be easily modified. Here we only discuss briefly what the changes are. Firstly, with

$$H\;=\;\left[\begin{array}{cccc}H_0&\cdots&H_{K-1}&\mathbf{0}\end{array}\right]$$

in mind, i.e. $H_{K_o-1}=\mathbf{0}$, the result of the squared Euclidean distance between $\bar{S}$ and $\bar{S}'$ appearing in (23) remains to hold. Similarly, the further-lower bounds on $d_E^2(\bar{S},\bar{S}')$ appearing in (29) and (37) stay without changes except that one should keep in mind that

1) the parameter m of the first case, where rank$(\bar{C}-\bar{C}')=mn_t$, and m out of K_o x_i's are distinct, has value from 1 up to $K_o-1=K$. This is because $H_{K_o-1}=\mathbf{0}$, hence we can always assume $x_{K_o-1}=x'_{K_o-1}$ without affecting the value of $d_E^2(\bar{S},\bar{S}')$. Thus the diversity gain resulting from the first case is
$$\min_{1\le m\le K}d^*_{mn_t,n_r}(mr).$$
compared to the case of odd K where (44) has m up to K_o.
2) the parameters m and n in the second case can be argued similarly as the above, and we have $1\le n<m\le K_o-1=K$. Hence the diversity gain resulting from this case is
$$\min_{1\le n\le K-1}d^*_{nn_t,n_r}(nr).$$

Therefore, overall the main result of the DMT optimality of the proposed construction remains to hold.

REFERENCES

[1] P. Elia, B. A. Sethuraman, and P. V. Kumar, "Perfect space-time codes for any number of antennas," *IEEE Trans. Inf. Theory*, vol. 52, no. 11, pp. 3853 – 3868, Nov. 2007.

[2] P. Elia, K. R. Kumar, S. A. Pawar, P. V. Kumar, and H.-F. Lu, "Explicit construction of space-time block codes achieving the diversity-multiplexing gain tradeoff," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3869–3884, Sep. 2006.

[3] H. F. Lu, "Explicit constructions of multi-block space-time codes that achieve the diversity-multiplexing tradeoff," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3790–3796, Aug. 2008.

[4] P. Elia and P. V. Kumar, "Approximately-universal space-time codes for the parallel, multi-block and cooperative-dynamic-decode-and-forward channels," Jul. 2007, http://arxiv.org/pdf/0706.3502.

[5] H. F. Lu, "Explicit constructions of multi-block space-time codes that achieve the diversity-multiplexing tradeoff," in *Proc. 2006 IEEE Int. Symp. Inform. Theory*, Seattle, WA, Jul. 2006, pp. 1149–1153.

[6] S. Yang and J.-C. Belfiore, "Optimal space-time codes for the amplify-and-forward cooperative channel," in *Proc. 43nd Allerton Conference on Communication, Control and Computing*, Monticello, Illinois, Sep. 2005.

[7] L. Zheng and D. Tse, "Diversity and multiplexing: a fundamental tradeoff in multiple antenna channels," *IEEE Trans. Inf. Theory*, vol. 49, no. 5, pp. 1073–1096, May 2003.

[8] R. A. Horn and C. R. Johnson, *Matrix Analysis*. Cambridge, UK: Cambridge University Press, 1985.