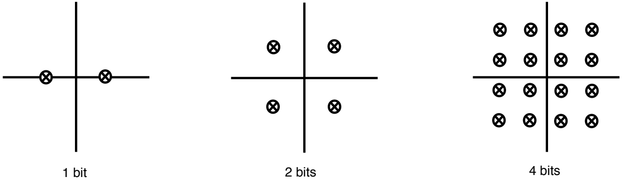
Random Matrices in Communication Theory

Rajesh Sundaresan

27 April 2011

Message transmission: an abstraction

- K transmit antennas sending messages
- Message is a signal $x_k \in S \subset \mathbb{C}^K$ carried on antenna k



- Each message is equiprobable
- Message requires energy $\mathbb{E}[|x_k|^2]$
- Can scale the constellation S

Impairments to transmitted signal

- L receive antennas
- Channel gain from transmit antenna k to receive antenna l is H_{lk}
- Received signal:
$$y = Hx + z$$
- $H \in \mathbb{C}^{L \times K}$, $z \in \mathbb{C}^{L}$
- H: random - iid entries distributed as $\mathbb{CN}(1)$, but realisation learnable at the receiver
- z: random - $\mathbb{CN}(I_L)$

- x: random - equiprobable in the message set with $\mathbb{E}[\|x\|^2] \leq P$ (battery life versus performance)
- Same constellation on each antenna $\Rightarrow \mathbb{E}[|x_k|^2] \leq P/K = p$.

How do these impairments arise

Random H with iid $\mathbb{CN}(1)$ entries:

- Arises because of scattering and many multipaths, with no dominant contribution from a single path
- No direct line of sight path
- If direct line of sight, mean is nonzero – also of interest, but not considered here

Random z: Receiver thermal noise in the receiving antenna

I: Receiver problem - MMSE

- Given y and H, process it and identify x
- Test each hypothesis for x, pick the most likely one (after having observed y and H). Exponential complexity. Want simpler receivers
- E.g., A linear receiver that minimises mean squared error (MMSE)

$$\rho := \min_{M \in \mathbb{C}K \times L} \mathbb{E}\left[\|x - My\|^2 \mid H\right]$$

Questions:
Find the argmin M_{opt}. It can depend on H.
Find ρ

The solution

Proposition:

- $M_{\text{opt}} = p\ H^* \left[I_L + pHH^*\right]^{-1}$,
- $\rho = p \operatorname{tr}\left\{(I_L + pHH^*)^{-1}\right\}$.

Observations:

- One random environment H. The optimal receiver can depend on H.
- Scaling very natural for the problem:

$$\rho = \frac{P}{K} \sum_{k=1}^{K} \frac{1}{1 + P\lambda_k\left(\frac{H^*H}{K}\right)}$$

- Just a scaled Stieltjes transform evaluated at a point.

Proof steps: standard fare in estimation

- If x were Gaussian, the best estimate is $\mathbb{E}[x|y]$, a linear estimate.
- Even otherwise, look for the best estimate within the affine family (Wiener-Kolmogorov filtering)
- Projection of x onto the affine family
- Let $\mathbb{E}[x] = 0$. Then

$$\begin{aligned} M_{\text{opt}} &= \left(\mathbb{E}[xy^*]\right)\left(\mathbb{E}[yy^*]\right)^{-1} \\ &= pH^*\left[I_L + pHH^*\right]^{-1} \end{aligned}$$

- MMSE (ρ) evaluation is by direct substitution.

The Marcenko-Pastur law

Theorem: Let L_K be the ESD of H^*H/K, and $\overline{L}_K$ its expectation. The entries are iid, zero mean, with variance 1 and bounded fourth moments. Let $L/K \to \beta$. Then

$$\begin{aligned} L_K &\overset{P}{\to} \mu_{MP} \\ \overline{L}_K &\to \mu_{MP} \end{aligned}$$

Proof: The tough exercise via Stieltjes transforms with the antidiagonal trick that I didn't do.

The law μ_{MP} has generalised density

$$f_\beta(x) = (1-\beta)^+ \, \delta(x) + \frac{\sqrt{(x-a)^+(b-x)^+}}{2\pi x}$$

where $a = (1-\sqrt{\beta})^2$ and $b = (1+\sqrt{\beta})^2$.

Observations: Mass at 0 and bounded support

II : CDMA for Code division multiple access

- K mobiles, each having a message to transmit
- The message x_k for the mobile k is "spread" over L symbols
- Transmit $x_k[H_{1k} \; H_{2k} \; \dots \; H_{Lk}]$ in the L symbols (signature)
- Superposition:

$$y = \sum_{k=1}^{K} \begin{bmatrix} H_{1k} \\ H_{2k} \\ \vdots \\ H_{Lk} \end{bmatrix} x_k + z = Hx + z$$

The twist: H_{lk} randomly picked from ± 1 with equal probability, independent of all others. Then normalised.

- Receiver informed (*pseudo noise* random bit generator)
- Helps hide information if seed is not known
- Use MMSE again. The same as the previous problem, with expectation over H as well.

III: The best code and Shannon capacity

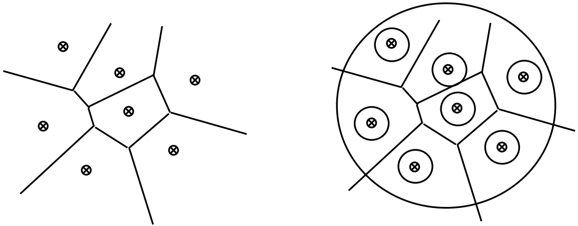
Code across time and exploit the law of large numbers. (Shannon 1948)

- $y(t) = H(t)x(t) + z(t)$, for $t = 1, 2, \ldots, T$.
- For now, fix $H(t) = H$, fixed for all t, known.
- Code: Messages are $\{1, 2, \ldots, M\}$. Each message maps to a position that the transmitter takes.

$$w \mapsto x^{(w)} \in (\mathbb{C}^K)^T$$

- Noise corrupts this and receiver gets corrupted $y \in (\mathbb{C}^L)^T$.
- Receiver should make probability of error arbitrarily small.
- What is $\log_2 M$ (bits per T symbols)? What is the rate $T^{-1}\log_2 M$? Maximum asymptotic rate? (Capacity)?

The scalar case $H \in \mathbb{C}$: $K = L = 1$



- Noise vector concentrates with a radius $\sqrt{T}$
- All noise spheres around message points disjoint
- All noise spheres are within radius $\sqrt{T(|H|^2 P + 1)}$ (Near orthogonality)
- $M \leq \frac{\alpha_{2T}\left(\sqrt{T(|H|^2P+1)}\right)^{2T}}{\alpha_{2T}\left(\sqrt{T}\right)^{2T}} = (1 + |H|^2 P)^T$
- Yields rate is at most $T^{-1} \log M \leq \log(1 + |H|^2 P)$.
- Can show that this is indeed *achievable*

Multiple antennas?

Theorem: Let $\{H(t)\}$ is stationary and ergodic. Let H denote $H(1)$. Under sufficient regularity on this process, the capacity per transmit antenna is given by

$$\begin{aligned} C_K &= \mathbb{E}\left[K^{-1}\log\det(I_L + pHH^*)\right] \\ &= \mathbb{E}\left[K^{-1}\sum_{k=1}^{K}\log\left(1 + P\lambda_k\left(\frac{HH^*}{K}\right)\right)\right] \end{aligned}$$

for a scenario where receiver knows $H(\cdot)$ and transmitter knows only its distribution. The unit is bits/symbol/antenna.

Evaluation

For Gaussian entries and finite K:

- Density $\propto \Delta(\lambda)^2 \exp\{-\sum_i \lambda_i\} \prod_i \lambda_i^{|K-L|}$
- Laguerre polynomials play the role of Hermite polynomials
- $p_{\lambda_1}(\lambda_1) = \frac{1}{m} \sum_{i=1}^{m} \phi_i(\lambda_1)^2 \lambda_1^{|K-L|} e^{-\lambda_1}$.
- Enables evaluation.

Asymptotic case as $K \to \infty$, we have

$$C_K = \int_0^\infty \log(1 + P\lambda)\ d\overline{L}_K(\lambda) \to \int_0^\infty \log(1 + P\lambda)\ d\mu_{MP}(\lambda).$$

$\log(1 + \cdot)$ is not bounded, but exploit monotonicity and concavity. See a later slide.

IV: The random environment case

- Design a code with a certain rate R.
- Encounter a random environment H.
- Can have a failed transmission with probability

$$
\begin{aligned}
&\Pr\left\{\int \log(1+P\lambda)\, dL_K(\lambda) < R\right\} \\
&= \Pr\left\{K^{-1}\sum_{k=1}^{K}\log\left(1+P\lambda_k\left(\frac{HH^*}{K}\right)\right) < R\right\}.
\end{aligned}
$$

For this to converge to 0, need convergence in probability to a constant c, and $R < c - \varepsilon$.

Convergence in probability

Theorem: Let $\xi_K = \int \log(1 + P\lambda)\ dL_K(\lambda)$. Then

$$\xi_K \xrightarrow{P} c = \int \log(1 + P\lambda)\ d\mu_{MP}(\lambda).$$

Proof: There is a common prob. space where $L_K \to \mu_{MP}$ a.s. (Skorohod). Consider the good set.
Let $\lambda^{(K)}$ be according to prob. measure L_K with distribution F_K.
Let G_K be distribution of $h(\lambda^{(K)}) := \log\left(1 + P\lambda^{(K)}\right)$.

$$\begin{aligned}\xi_K &= \int g\ dG_K(g) = \int [1 - G_K(g)]dg = \int [1 - F_K(h^{-1}(g))]dg \\ &= \int [1 - F_K(\lambda)]h'(\lambda)\ d\lambda\end{aligned}$$

Apply BCT and ($F_K \to F$ a.e) to get $\xi_K \to c$ a.s.
So $\xi_K \to c$ in distribution, which also holds in the original space.
Convergence in distribution to a constant implies convergence in probability.

Variations

- Fluctuation result:

$$\Pr\left\{\sum_{k=1}^{K}\log\left(1+P\lambda_k\left(\frac{HH^*}{K}\right)\right)<Kc-u\right\}\to\Phi(u;\sigma^2)$$

- $y = HAx + z$, where A is a diagonal matrix. Correlations introduced.
- $H = U_r H_w U_t^*$
- Instead of $K_X = (P/K)I_K$, can tune K_X to H, if transmitter also has knowledge of the channel condition. This is not absurd in some cases.

References

- I.E.Telatar, "Capacity of multiantenna Gaussian channels," *Eur. Trans. Telecommun. Rel. Technol.*, vol. 10, no. 6, pp. 585-59, Nov. 1999.
- S. Verdú and S. Shamai, "Spectral efficiency of CDMA with random spreading," *IEEE Trans. on Inf. Theory*, vol. 45, no. 2, pp. 622-620, Mar. 1999.
- A. M. Tulino and S. Verdú, Random Matrix Theory and Wireless Communications, Foundations and Trends in Commun. and Inf. Theory, vol. 1, no. 1, pp. 1-182, 2004, and references therein.