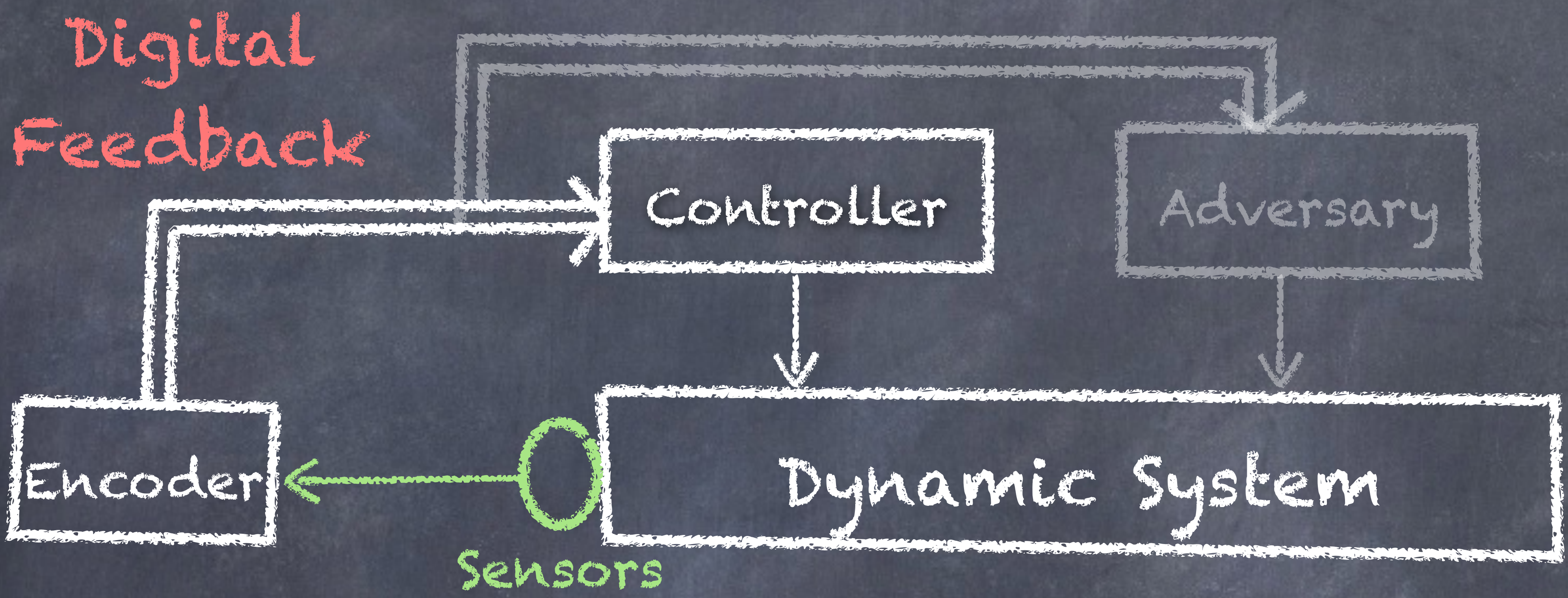
Secure Rate-Limited Feedback for Control

Paul Cuff and Sai Satpathy

Control Setting



1. Derive "data-rate theorem" from heuristic (channel synthesis)
2. Generalize heuristic for security
3. Apply heuristic for secure data-rate theorem

Linear Control Theory

- State dynamics: $x_{n+1} = Ax_n + Bu_n + w_n$
- Sensors: $y_n = Cx_n + v_n$

Gaussian

- Cost: $J(U) = E\ 1/N\ \Sigma_n\ x_n^T Q x_n + u_n^T S u_n$
- Optimal Control:
  - Estimation (Kalman)
  - Control (LQR)
  - Performance (Riccati)

"Stable" if the steady state cost is finite

Linear Control Theory

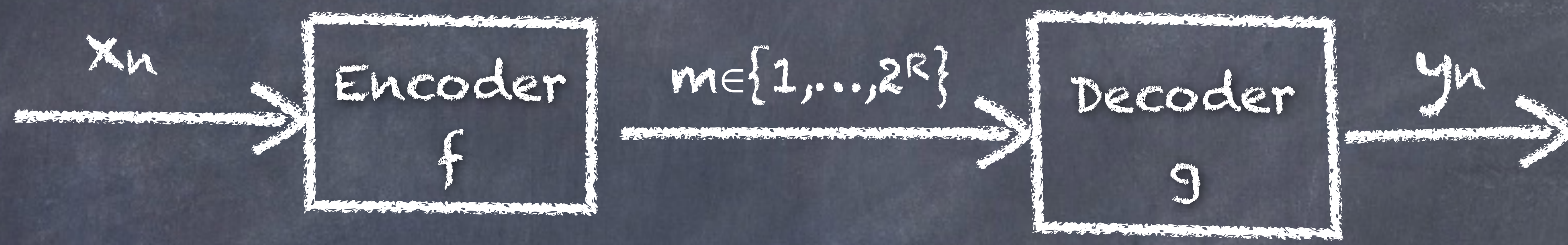
- State dynamics: $x_{n+1} = Ax_n + \cancel{B}u_n + w_n$
- Sensors: $y_n = \cancel{C}x_n + v_n$

Gaussian

- Cost: $J(U) = E\ 1/N \sum_n x_n^T Q x_n + \cancel{u_n^T S} u_n$
- Optimal Control:
  - Estimation (Kalman)
  - Control (LQR)
  - Performance (Riccati)

"Stable" if the steady state cost is finite

Digital Feedback

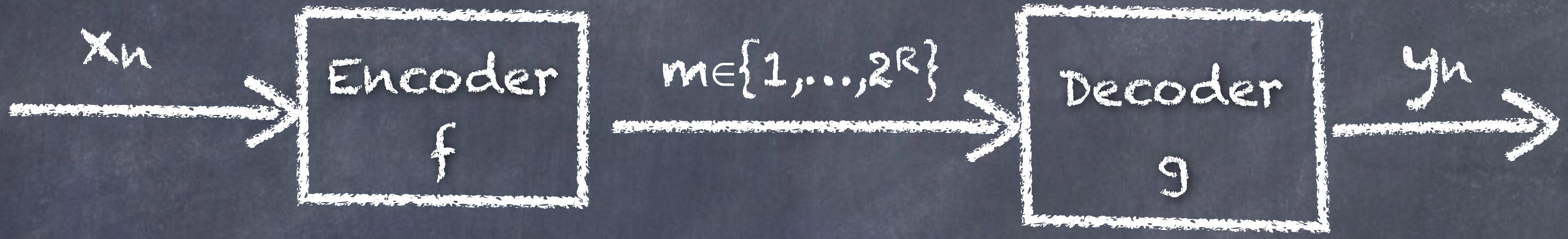


- State dynamics: $x_{n+1} = Ax_n + Bu_n + w_n$
- Feedback: $y_n = g(f(x_n)),\ f_n \in [2^R]$
- Cost: $J(U) = E\ 1/N\ \Sigma_n\ x_n^T Q x_n + u_n^T S u_n$

Data-rate Theorem

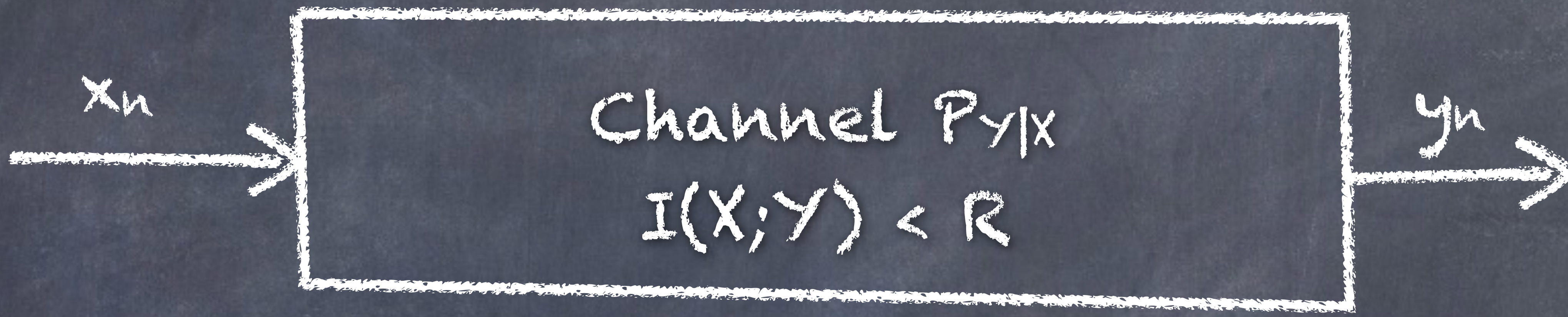
- Necessary and sufficient condition for stability:
  - $R > \sum \log |\lambda_i|$
  - λ_i are the unstable eigenvalues of A
- [Nair, Evans, Fagnani, Zampieri], [Tatikonda, Mitter]
- Proof:
  - uniform scalar quantization in unstable dimensions
  - zoom-in, zoom-out
  - uncertainty analysis

Channel Synthesis



- $R > I(X_n;Y_n)$ (data processing ineq.)
- Assume this is the only constraint:
  - Let $P_{Y|X}$ be any channel satisfying the mutual information constraint

Channel Synthesis



- $R > I(X_n;Y_n)$ (data processing ineq.)
- Assume this is the only constraint:
  - Let $P_{Y|X}$ be any channel satisfying the mutual information constraint

Gaussian Channel

- State dynamics: $x_{n+1} = Ax_n + u_n + w_n$
- Sensors (feedback): $y_n = x_n + v_n$

Channel noise variance depends on rate R and variance of x_n

Scalar: $\sigma_v^2 = \sigma_x^2 / (2^{2R} - 1)$

- Optimal control: $u_n = -A\xi_n$
  - ξ_n is the best estimate of x_n,
  - Innovation Process: $\zeta_n = x_n - \xi_n$
  - State dynamics: $x_{n+1} = A\,\zeta_n + w_n$

Same Threshold

- Necessary and Sufficient
  - $R > \Sigma \log |\lambda_i|$
- Analysis: Riccati equations (scalar)
  - $\sigma_{\zeta,n+1}^2 = (a^2\sigma_{\zeta,n}^2 + \sigma_w^2)2^{-2R}$
  - Steady state: $\sigma_\zeta^2 = \sigma_w^2/(2^{2R} - a^2)$

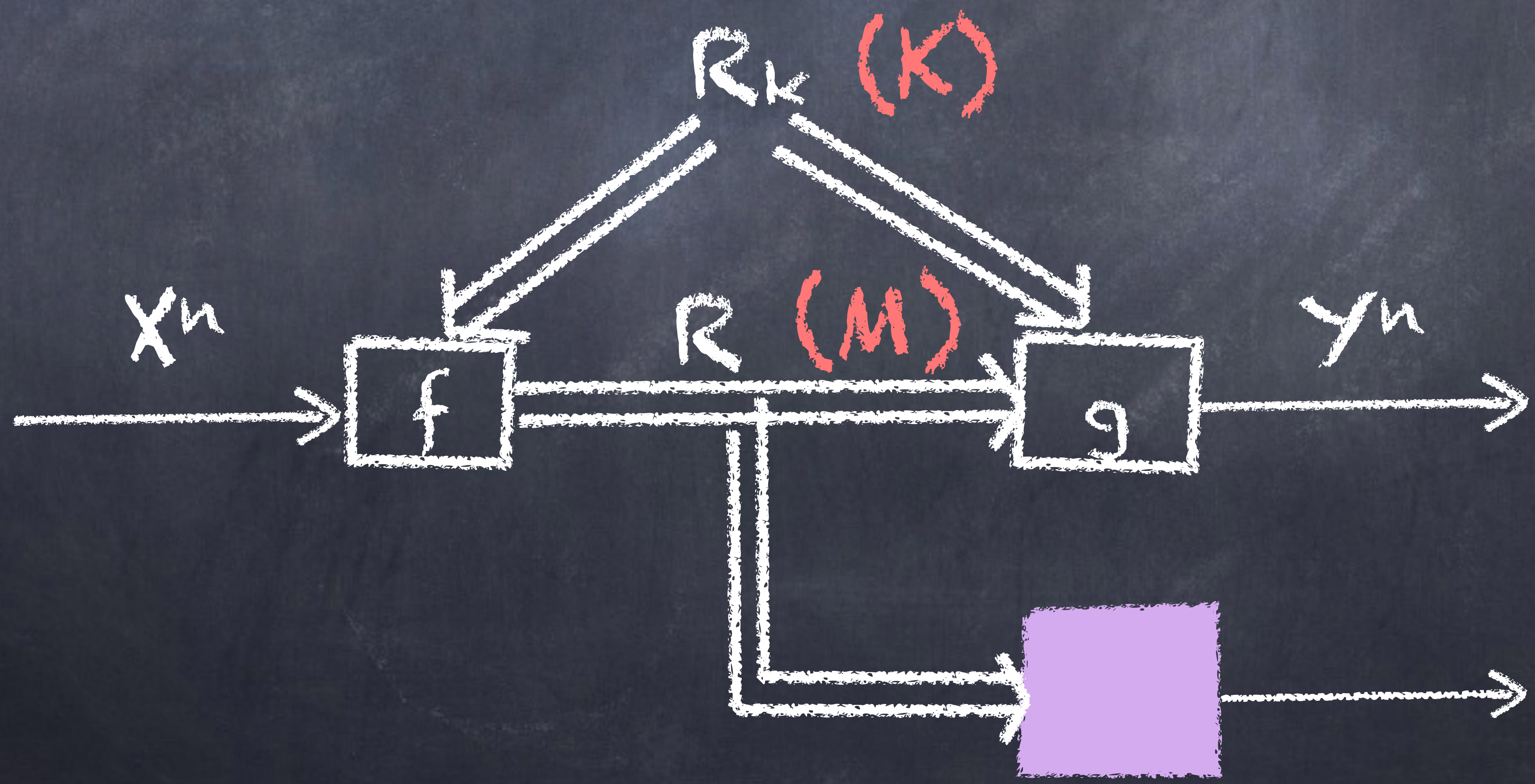
Similar Steady State Performance

$$J \geq d\, |\Sigma_w|^{1/d}\, 2^{-2R/d} / (1 - 2^{-2(R - \log|A|)/d})$$

Similar to [Nair-Evans 04]

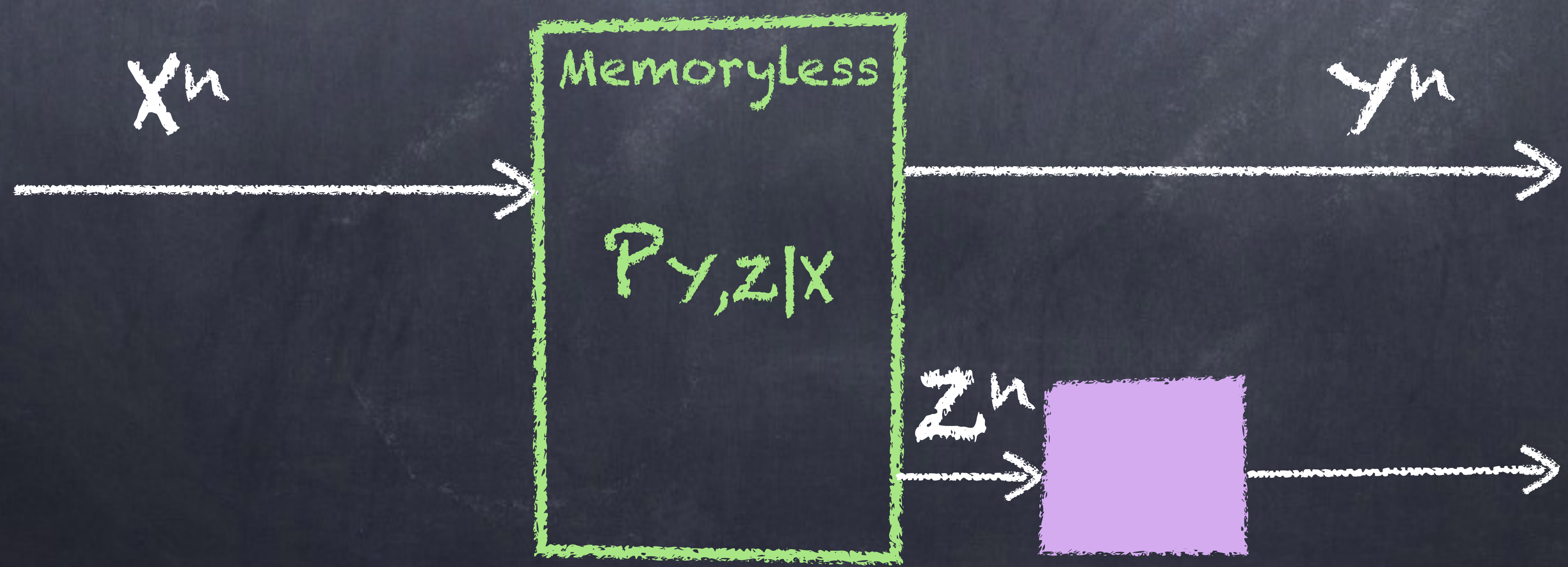
Synthetic noise

- Communication with secret key



Synthetic noise

- Communication with secret key



Synthetic noise

- Communication with secret key

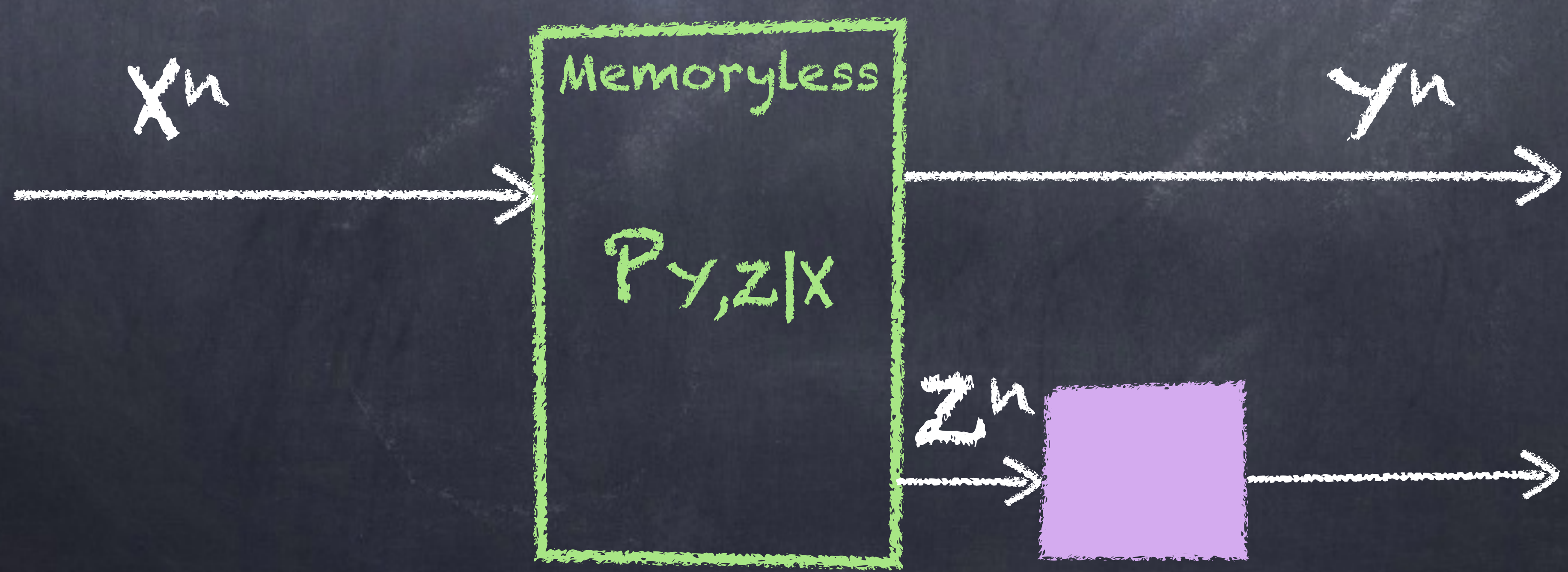
[Schieler-C 13]

Constraints:

$R > I(X;VZ)$,

$R_k > I(XY;V|Z)$,

$X - (V,Z) - Y$



Synthetic Gaussian Channel

- (wlog) Physically degraded:
  - $y_n = x_n + v_{1,n}$
  - $z_n = y_n + v_{2,n}$

independent noise

- Optimization of V: Jointly Gaussian
- (wlog) Markov chain: X-V-Y-Z

because Gaussian

Rate requirements

$X \rightarrow Y \rightarrow Z$

ρ_y between X and Y

ρ_z between X and Z

- Effective correlation:
  - $\alpha = \sqrt{(\rho_y^2 - \rho_z^2)/(1-\rho_z^2)}$
- Required rates (for high R):
  - (comm.) $R > I(\alpha) + I(\rho_z) + 1/2 \log(1+\alpha)$
  - (key) $R_k > C(\alpha) = I(\alpha) + \log(1+\alpha)$

Gaussian mutual information: $I(x) = 1/2 \log(1/(1-x^2))$

Apply heuristic

- Adversary observes z_n
- State dynamics: $x_{n+1} = Ax_n + u_n(y^n) + \underbrace{v_n(z^n)}_{\text{Adversary's disturbance signal}} + w_n$
- Restriction:
  - Adversary only removes best estimate of u_n
  - Equivalently, uses best estimate of the state to undo the control

Result (scalar)

- Let R' be the non-secure required rate ($R' = \log |a|$)
- Required rates for stability (high R):
  - $R > R' + 1/2 \log(1 + \sqrt{(1-2^{-2R'})})$
  - $R_k > R' + \log(1 + \sqrt{(1-2^{-2R'})})$

Summary

- Optimistic heuristic for quantization (joint dist. only constrained by MI)
- Crisply recovers "data-rate theorem"
- Gaussian optimization of secure channel synthesis
- Some fun with secure control