Phase Transitions of Random Codes and GV-Bounds

Yun Fan

Math Dept, CCNU

A joint work with Ling, Liu, Xing

Oct 2011

Phase Transitions of Random Codes and GV-Bounds

Phase Transitions: in Physics

Phase Transitions: in Physics

$$\text{SOLID} \xrightleftharpoons[\text{freezing}]{\text{melting}} \text{LIQUID} \xrightleftharpoons[\text{condensation}]{\text{vaporization}} \text{GAS}$$

$$0^{o}\text{C} \qquad\qquad\qquad 100^{o}\text{C}$$

Phase Transitions in Mathematics: Pioneer

Random graph: $G(n, p)$

n vertices

to each pare of two vertices an edge is settled at probability p

Phase Transitions in Mathematics: Pioneer

Random graph: $G(n, p)$

n vertices

to each pare of two vertices an edge is settled at probability p

$n = 2$		
probability	$1 - p$	p

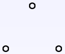
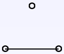
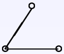
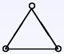
Phase Transitions in Mathematics: Pioneer

Random graph: $G(n, p)$

n vertices

to each pare of two vertices an edge is settled at probability p

$n = 2$		
probability	$1 - p$	p

$n = 3$				
probability	$(1 - p)^3$	$3(1 - p)^2 p$	$3(1 - p)p^2$	p^3

Phase Transitions in Mathematics: Pioneer

Is $G(n, p)$ connected ?

Phase Transitions in Mathematics: Pioneer

Is $G(n, p)$ connected ?

$$\text{DISCONNECTED} \quad \underset{\substack{p \text{ decreasing} \\ \frac{\ln n}{n}}}{\overset{\substack{\frac{\ln n}{n} \\ p \text{ increasing}}}{\rightleftarrows}} \quad \text{CONNECTED}$$

Phase Transitions in Mathematics: Pioneer

$$\lim_{n\to\infty} \Pr\left(G(n,p) \text{ connected}\right) = \begin{cases} 0, & p < \frac{\ln n}{n}; \\ 1, & p > \frac{\ln n}{n}. \end{cases}$$

Phase Transitions in Mathematics: Pioneer

$$\lim_{n\to\infty} \Pr\left(G(n,p) \text{ connected}\right) = \begin{cases} 0, & p < \frac{\ln n}{n}; \\ 1, & p > \frac{\ln n}{n}. \end{cases}$$

published in:

P. Erdös, A. Rényi, “On the evolution of random graphs”, *Publ. Math. Inst. Hungar. Acad. Sci.* vol.5, pp17-61, 1960.

Phase Transitions in Mathematics: Pioneer

$$\lim_{n\to\infty} \Pr\left(G(n,p) \text{ connected}\right) = \begin{cases} 0, & p < \frac{\ln n}{n}; \\ 1, & p > \frac{\ln n}{n}. \end{cases}$$

published in:

P. Erdös, A. Rényi, "On the evolution of random graphs", *Publ. Math. Inst. Hungar. Acad. Sci.* vol.5, pp17-61, 1960.

usage "phase transition" in Mathematics appeared first time in:

S.Janson, T.Luczak, and A.Rucinski, "The Phase Transition" Ch.5 in *Random Graphs*, New York: Wiley, pp. 103-138, 2000.

Phase Transitions in Mathematics: Linear system

Random linear system S over a finite filed F:

$$S: \quad \begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \quad \cdots \qquad \cdots \qquad \cdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m \end{cases}$$

Phase Transitions in Mathematics: Linear system

Random linear system S over a finite filed F:

$$S: \quad \begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \quad \cdots \qquad \cdots \qquad \cdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m \end{cases}$$

$$\lim_{n\to\infty} \Pr\left(S \text{ has solutions}\right) = \begin{cases} 1, & r < 1; \\ 0, & r > 1. \end{cases} \qquad \text{where } r = \frac{m}{n}$$

Phase Transitions in Mathematics: Linear system

Random linear system S over a finite filed F:

$$S: \quad \begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \quad \cdots \qquad\quad \cdots \qquad\quad \cdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m \end{cases}$$

$$\lim_{n\to\infty} \Pr\left(S \text{ has solutions}\right) = \begin{cases} 1, & r < 1; \\ 0, & r > 1. \end{cases} \qquad \text{where } r = \frac{m}{n}$$

$$\text{SOLUTION} \; \begin{array}{c} 1 \\ \xrightarrow{r \text{ increasing}} \\ \xleftarrow[r \text{ decreasing}]{} \\ 1 \end{array} \; \text{NO SOLUTION}$$

Phase Transitions in Mathematics: Linear system

A proof

Phase Transitions in Mathematics: Linear system

A proof

$$A = (a_{ij})_{m\times n} = \big(A_1|\cdots|A_n\big), \quad \mathbf{b} = (b_1, \cdots, b_m)^T.$$

Phase Transitions in Mathematics: Linear system

A proof

$$A = (a_{ij})_{m\times n} = \big(A_1|\cdots|A_n\big), \quad \mathbf{b} = (b_1, \cdots, b_m)^T.$$

$r < 1$

$$\begin{aligned}\Pr\big(\mathrm{rank} A < m\big) &\le \sum_{W \le F^m, \dim W = m-1} \Pr\big(\text{all } A_j \text{ contained in } W\big)\\ &\le q^m \cdot (1/q)^n = q^{(r-1)n} \longrightarrow 0.\end{aligned}$$

$$\lim_{n\to\infty} \Pr\big(\text{solution}\big) \ge \lim_{n\to\infty} \Pr\big(\mathrm{rank} A = m\big) = 1$$

Phase Transitions in Mathematics: Linear system

A proof

$$A = (a_{ij})_{m\times n} = \left(A_1|\cdots|A_n\right), \quad \mathbf{b} = (b_1, \cdots, b_m)^T.$$

$r < 1$

$$\begin{aligned}\Pr\left(\mathrm{rank} A < m\right) &\leq \sum_{W\leq F^m, \dim W = m-1} \Pr\left(\text{all } A_j \text{ contained in } W\right) \\ &\leq q^m \cdot (1/q)^n = q^{(r-1)n} \longrightarrow 0.\end{aligned}$$

$$\lim_{n\to\infty} \Pr\left(\text{solution}\right) \geq \lim_{n\to\infty} \Pr\left(\mathrm{rank} A = m\right) = 1$$

$r > 1$

$$\begin{aligned}\Pr\left(\text{solution}\right) &= \Pr\left(\mathbf{b} \in \mathrm{Span}(A_1, \cdots, A_n)\right) \\ &\leq q^n/q^m = q^{(1-r)n} \longrightarrow 0.\end{aligned}$$

Shannon's World

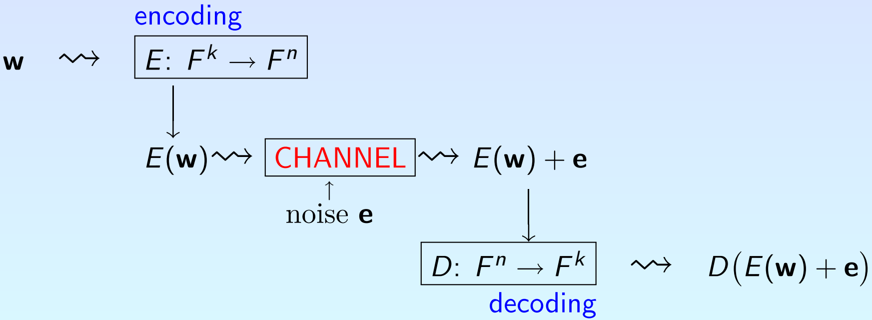
F: alphabet, cardinality $|F| = q$.

Message $\rightsquigarrow$ word $\mathbf{w} \in F^k$

Shannon's World

F: alphabet, cardinality $|F| = q$.

Message $\rightsquigarrow$ word $\mathbf{w} \in F^k$



encoding

$\mathbf{w} \rightsquigarrow \boxed{E\colon F^k \to F^n}$

$\downarrow$

$E(\mathbf{w}) \rightsquigarrow \boxed{\text{CHANNEL}} \rightsquigarrow E(\mathbf{w}) + \mathbf{e}$

$\uparrow$

noise $\mathbf{e}$

$\downarrow$

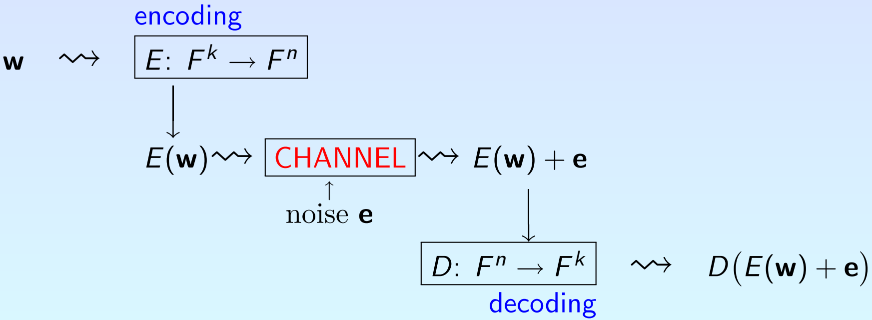
$\boxed{D\colon F^n \to F^k} \rightsquigarrow D\big(E(\mathbf{w}) + \mathbf{e}\big)$

decoding

Shannon's World

F: alphabet, cardinality $|F| = q$.

Message $\rightsquigarrow$ word $\mathbf{w} \in F^k$



encoding

$$\mathbf{w} \rightsquigarrow \boxed{E\colon\ F^k \to F^n}$$

$$E(\mathbf{w}) \rightsquigarrow \boxed{\text{CHANNEL}} \rightsquigarrow E(\mathbf{w}) + \mathbf{e}$$

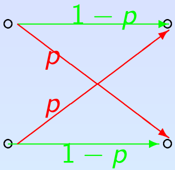
$\uparrow$ noise $\mathbf{e}$

$$\boxed{D\colon\ F^n \to F^k} \rightsquigarrow D\big(E(\mathbf{w}) + \mathbf{e}\big)$$

decoding

Does $D\big(E(\mathbf{w}) + \mathbf{e}\big) = \mathbf{w}$?

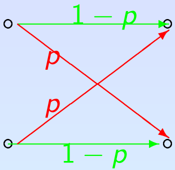
Shannon's World: Binary symmetric channels



p=false probability

$1-p$=true probability

Shannon's World: Binary symmetric channels

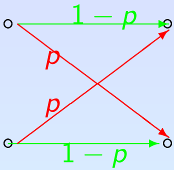


p=false probability

$1-p$=true probability

Transition probability matrix: $\begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix}$

Shannon's World: Binary symmetric channels



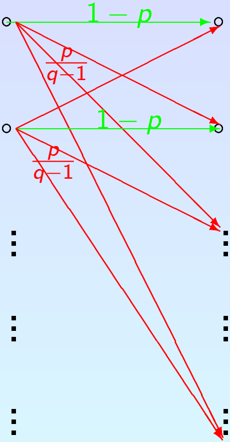
p=false probability

$1-p$=true probability

Transition probability matrix: $\begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix}$

Entropy: $H(p) = -p\log_2 p - (1-p)\log_2(1-p)$

Shannon's World: q-ary symmetric channels



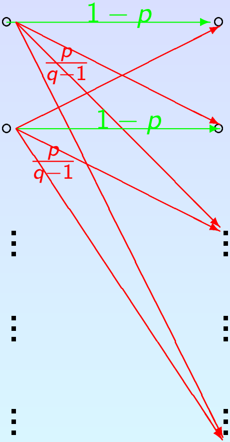
$p =$ false probability

$1 - p =$ true probability

transition probability matrix:

$$\begin{pmatrix} 1-p & \frac{p}{q-1} & \cdots & \frac{p}{q-1} \\ \frac{p}{q-1} & 1-p & \cdots & \frac{p}{q-1} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{p}{q-1} & \frac{p}{q-1} & \cdots & 1-p \end{pmatrix}$$

Shannon's World: q-ary symmetric channels



$p =$ false probability

$1 - p =$ true probability

transition probability matrix:

$$\begin{pmatrix} 1-p & \frac{p}{q-1} & \cdots & \frac{p}{q-1} \\ \frac{p}{q-1} & 1-p & \cdots & \frac{p}{q-1} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{p}{q-1} & \frac{p}{q-1} & \cdots & 1-p \end{pmatrix}$$

q-ary Entropy: $H_q(p) = \log_q(q-1) - p\log_q p - (1-p)\log_q(1-p)$

Shannon's World: Shannon's Theorem

Coding device $= \boxed{\boxed{E : F^k \to F^n} + \boxed{D : F^n \to F^k}}$

Rate $r = k/n$

Shannon's World: Shannon's Theorem

$$\text{Coding device} = \boxed{\boxed{E : F^k \to F^n} + \boxed{D : F^n \to F^k}}$$

Rate $r = k/n$

Shannon's Theorem

If $r < 1 - H_q(p)$ then there exists a coding device of rate r such that

$$\lim_{n \to \infty} \Pr\left(D\left(E(\mathbf{w}) + \mathbf{e}\right) = \mathbf{w}\right) = 1.$$

If $r > 1 - H_q(p)$ then, for any coding device of rate r,

$$\lim_{n \to \infty} \Pr\left(D\left(E(\mathbf{w}) + \mathbf{e}\right) = \mathbf{w}\right) = 0.$$

Shannon's World: Shannon's Theorem

$c = 1 - H_q(p)$: the *capacity* of the q-ary symmetric channel.

Shannon's World: Shannon's Theorem

$c = 1 - H_q(p)$: the *capacity* of the q-ary symmetric channel.

$$\text{HIGH FIDELITY} \;\; \underset{\substack{r \text{ decreasing} \\ c}}{\overset{\substack{c \\ r \text{ increasing}}}{\rightleftarrows}} \;\; \text{NO FIDELITY}$$

Shannon's World: Shannon's Theorem

C. E. Shannon, "A mathematical theory of communication", *Bell Sys. Tech. Journal*, vol.27, pp379-423, 623C655, 1948.

If $r < c$, $\lim_{n\to\infty} \Pr\big(D\big(E(\mathbf{w}) + \mathbf{e}\big) = \mathbf{w}\big) = 1$.

If $r > c$, there is a $b < 1$ such that $\lim_{n\to\infty} \Pr\big(D\big(E(\mathbf{w}) + \mathbf{e}\big) = \mathbf{w}\big) < b$.

Shannon's World: Shannon's Theorem

C. E. Shannon, "A mathematical theory of communication", *Bell Sys. Tech. Journal*, vol.27, pp379-423, 623C655, 1948.

If $r < c$, $\lim_{n\to\infty} \Pr\big(D\big(E(\mathbf{w}) + \mathbf{e}\big) = \mathbf{w}\big) = 1.$

If $r > c$, there is a $b < 1$ such that $\lim_{n\to\infty} \Pr\big(D\big(E(\mathbf{w}) + \mathbf{e}\big) = \mathbf{w}\big) < b.$

Jacob Wolfowitz, "The coding of messages subject to chancs errors", *Illinois J. Math.*, vol.1, pp591-606, 1957.

If $r > c$, $\lim_{n\to\infty} \Pr\big(D\big(E(\mathbf{w}) + \mathbf{e}\big) = \mathbf{w}\big) = 0.$

Hamming's World

Hamming distance: $d_H(\mathbf{x}, \mathbf{x}') = |\{1 \leq i \leq n \mid x_i \neq x_i'\}|, \quad \mathbf{x}, \mathbf{x}' \in F^n$

Codes: $C \subseteq F^n$

rate: $R(C) = \log_q(|C|)/n$, i.e. $|C| = F^{R(C)n}$

minimal distance: $d_H(C) = \min_{\mathbf{c} \neq \mathbf{c}' \in C} d_H(\mathbf{c}, \mathbf{c}')$

relative distance: $\delta_H(C) = d_H(C)/n$

Hamming's World

Hamming distance: $d_H(\mathbf{x}, \mathbf{x}') = |\{1 \le i \le n \mid x_i \ne x'_i\}|, \quad \mathbf{x}, \mathbf{x}' \in F^n$

Codes: $C \subseteq F^n$

rate: $R(C) = \log_q(|C|)/n, \quad$ i.e. $|C| = F^{R(C)n}$

minimal distance: $d_H(C) = \min_{\mathbf{c} \ne \mathbf{c}' \in C} d_H(\mathbf{c}, \mathbf{c}')$

relative distance: $\delta_H(C) = d_H(C)/n$

Linear codes: if F is a finite field, and C is a subspace of F^n

weight: $w_H(\mathbf{x}) = |\{1 \le i \le n \mid x_i \ne 0\}|$

minimal weight: $w_H(C) = \min_{\mathbf{0} \ne \mathbf{c} \in C} w_H(\mathbf{c})$

$$d_H(C) = w_H(C)$$

Hamming's World: Good codes

Good C: $R(C)$ is large, and $\delta_H(C)$ is large

Hamming's World: Good codes

Good C: $R(C)$ is large, and $\delta_H(C)$ is large

Trade off between rate and relative distance ?

Hamming's World: Upper bounds

Let $\delta_0 = 1 - q^{-1}$

Given $\delta_H(C) = \delta, \quad 0 < \delta < \delta_0$

Hamming's World: Upper bounds

Let $\delta_0 = 1 - q^{-1}$

Given $\delta_H(C) = \delta, \quad 0 < \delta < \delta_0$

Many functions bound up $r = R(C)$:

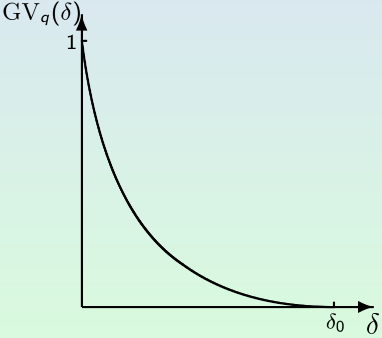
Singleton bound:	$r \le 1 - \delta$
Plotkin bound:	$r \le 1 - \frac{\delta}{\delta_0}$
Hamming bound:	$r \le 1 - H_q(\frac{\delta}{2})$
Elias bound:	$r \le 1 - H_q(\delta_0 - \sqrt{\delta_0(\delta_0 - \delta)})$
...	...

Hamming's World: Lower bounds

When we are given $\delta_H(C) = \delta$, to explore good codes, we are in fact concerned with how large $r = R(C)$ could reach.

Gilbert-Varshamov Bound: Function $\mathrm{GV}_q(\delta)$

$$\mathrm{GV}_q(\delta) = 1 - H_q(\delta)\,, \qquad \delta \in (0, \delta_0)$$



Gilbert-Varshamov Bound: GV-bound

Asymptotic Gilbert-Varshamov Bound

For any $r < \mathrm{GV}_q(\delta)$, there exist codes C over F (of large enough length) with rate r and relative distance $> \delta$.

GV-bound: Gilbert's argument, greedy algorithm

$d = \delta n$, $k = rn$; $M = q^k$

$B(\mathbf{x}, d) =$the Hamming ball, $V_q(n, d) = |B(\mathbf{x}, d)|$

GV-bound: Gilbert's argument, greedy algorithm

$d = \delta n$, $k = rn$; $M = q^k$

$B(\mathbf{x}, d)$ =the Hamming ball, $V_q(n, d) = |B(\mathbf{x}, d)|$

- Take $\mathbf{c}_1 \in F^n$; take $\mathbf{c}_2 \in F^n - B(\mathbf{c}_1, d)$; $\cdots$

GV-bound: Gilbert's argument, greedy algorithm

$d = \delta n$, $k = rn$; $M = q^k$

$B(\mathbf{x}, d)$ =the Hamming ball, $V_q(n, d) = |B(\mathbf{x}, d)|$

- Take $\mathbf{c}_1 \in F^n$; take $\mathbf{c}_2 \in F^n - B(\mathbf{c}_1, d)$; $\cdots$
- once $F^n - \bigcup_{i=1}^{m} B(\mathbf{c}_i, d) \neq \emptyset$, take $\mathbf{c}_{m+1} \in F^n - \bigcup_{i=1}^{m} B(\mathbf{c}_i, d)$; $\cdots$

GV-bound: Gilbert's argument, greedy algorithm

$d = \delta n$, $k = rn$; $M = q^k$

$B(\mathbf{x}, d)$ =the Hamming ball, $V_q(n, d) = |B(\mathbf{x}, d)|$

- Take $\mathbf{c}_1 \in F^n$; take $\mathbf{c}_2 \in F^n - B(\mathbf{c}_1, d)$; $\cdots$
- once $F^n - \bigcup_{i=1}^{m} B(\mathbf{c}_i, d) \neq \emptyset$, take $\mathbf{c}_{m+1} \in F^n - \bigcup_{i=1}^{m} B(\mathbf{c}_i, d)$; $\cdots$
- up to $\bigcup_{i=1}^{M} B(\mathbf{c}_i, d) = F^n$.

GV-bound: Gilbert's argument, greedy algorithm

$d = \delta n$, $k = rn$; $M = q^k$

$B(\mathbf{x}, d) =$the Hamming ball, $V_q(n, d) = |B(\mathbf{x}, d)|$

- Take $\mathbf{c}_1 \in F^n$; take $\mathbf{c}_2 \in F^n - B(\mathbf{c}_1, d)$; $\cdots$
- once $F^n - \bigcup_{i=1}^{m} B(\mathbf{c}_i, d) \neq \emptyset$, take $\mathbf{c}_{m+1} \in F^n - \bigcup_{i=1}^{m} B(\mathbf{c}_i, d)$; $\cdots$
- up to $\bigcup_{i=1}^{M} B(\mathbf{c}_i, d) = F^n$.

- $M \cdot V_q(n, d) = \sum_{i=1}^{M} V_q(n, d) \geq \left| \bigcup_{i=1}^{M} B(\mathbf{c}_i, d) \right| = q^n$

GV-bound: Gilbert's argument, greedy algorithm

$d = \delta n$, $k = rn$; $M = q^k$

$B(\mathbf{x}, d)$ =the Hamming ball, $V_q(n, d) = |B(\mathbf{x}, d)|$

- Take $\mathbf{c}_1 \in F^n$; take $\mathbf{c}_2 \in F^n - B(\mathbf{c}_1, d)$; $\cdots$
- once $F^n - \bigcup_{i=1}^{m} B(\mathbf{c}_i, d) \neq \emptyset$, take $\mathbf{c}_{m+1} \in F^n - \bigcup_{i=1}^{m} B(\mathbf{c}_i, d)$; $\cdots$
- up to $\bigcup_{i=1}^{M} B(\mathbf{c}_i, d) = F^n$.

- $M \cdot V_q(n, d) = \sum_{i=1}^{M} V_q(n, d) \geq \left| \bigcup_{i=1}^{M} B(\mathbf{c}_i, d) \right| = q^n$
- $r = \log_q M/n \geq 1 - \log_q V_q(n, d)/n \approx 1 - H_q(\delta) = \mathrm{GV}_q(\delta)$

Varshamov's argument, probabilistic method

Varshamov

Select a linear code L of rate $r < \mathrm{GV}_q(\delta)$ uniformly at random from F^n where F is a finite field, then

$$\lim_{n \to \infty} \Pr(\delta_H(L) > \delta) = 1$$

Varshamov's argument, probabilistic method

Varshamov

Select a linear code L of rate $r < \mathrm{GV}_q(\delta)$ uniformly at random from F^n where F is a finite field, then

$$\lim_{n\to\infty} \Pr(\delta_H(L) > \delta) = 1$$

- Random linear map: $g : F^k \to F^n$, or, random matrix $G = (g_{ij})_{m\times n}$

Varshamov's argument, probabilistic method

Varshamov

Select a linear code L of rate $r < \mathrm{GV}_q(\delta)$ uniformly at random from F^n where F is a finite field, then

$$\lim_{n\to\infty} \Pr(\delta_H(L) > \delta) = 1$$

- Random linear map: $g : F^k \to F^n$, or, random matrix $G = (g_{ij})_{m\times n}$
- For any $\mathbf{0} \neq \mathbf{b} \in F^k$,
  $\Pr\left(w_H(g(\mathbf{b})) \leq d\right) = V_q(n,d)/q^n \approx q^{-\mathrm{GV}_q(\delta)n}$

Varshamov's argument, probabilistic method

Varshamov

Select a linear code L of rate $r < \mathrm{GV}_q(\delta)$ uniformly at random from F^n where F is a finite field, then

$$\lim_{n\to\infty} \Pr(\delta_H(L) > \delta) = 1$$

- Random linear map: $g : F^k \to F^n$, or, random matrix $G = (g_{ij})_{m\times n}$
- For any $\mathbf{0} \neq \mathbf{b} \in F^k$,
  $\Pr\left(w_H(g(\mathbf{b})) \leq d\right) = V_q(n,d)/q^n \approx q^{-\mathrm{GV}_q(\delta)n}$
- $$\Pr(\delta_H(C) \leq \delta) = \Pr\left(\bigcup_{\mathbf{0}\neq\mathbf{b}\in F^k} (w_H(g(\mathbf{b})) \leq d)\right)$$

Varshamov's argument, probabilistic method

Varshamov

Select a linear code L of rate $r < \mathrm{GV}_q(\delta)$ uniformly at random from F^n where F is a finite field, then

$$\lim_{n\to\infty} \Pr(\delta_H(L) > \delta) = 1$$

- Random linear map: $g : F^k \to F^n$, or, random matrix $G = (g_{ij})_{m\times n}$
- For any $\mathbf{0} \neq \mathbf{b} \in F^k$,
  $\Pr\left(w_H(g(\mathbf{b})) \leq d\right) = V_q(n,d)/q^n \approx q^{-\mathrm{GV}_q(\delta)n}$
- $$\Pr(\delta_H(C) \leq \delta) = \Pr\left(\bigcup_{\mathbf{0}\neq\mathbf{b}\in F^k} (w_H(g(\mathbf{b})) \leq d)\right)$$
- $$\Pr(\delta_H(C) \leq \delta) \leq q^k \cdot V_q(n,d)/q^n \leq q^{rn-\mathrm{GV}_q(\delta)n} \longrightarrow 0$$

GV-Bound: Comparison with Shannon's world

GV-Bound: Comparison with Shannon's world

- q-ary GV-bound coincides exactly with the Shannon's capacity of q-ary symmetric channels

GV-Bound: Comparison with Shannon's world

- q-ary GV-bound coincides exactly with the Shannon's capacity of q-ary symmetric channels
- Varshamov's argument deals with random objects by means of probabilistic methods

GV-Bound: Comparison with Shannon's world

- q-ary GV-bound coincides exactly with the Shannon's capacity of q-ary symmetric channels
- Varshamov's argument deals with random objects by means of probabilistic methods
- What happen if r is beyond GV-bound ?

GV-Bound: Beyond GV-bound

- Codes of relative distance $> \delta$ and rate r beyond GV-bound ?

GV-Bound: Beyond GV-bound

- Codes of relative distance $> \delta$ and rate r beyond GV-bound ?
  Famous work: Yes if $q \geq 49$, algebraic geometry codes

  M. A. Tsfasman, S.G. Vladuts, T. Zink, "Modular curves, Shimura curves and Goppa codes, better than Varshamov-Gilbert bound", *Math. Nachrichten*, vol.104, pp.13-28, 1982.

GV-Bound: Beyond GV-bound

- Codes of relative distance $> \delta$ and rate r beyond GV-bound ?

  Famous work: Yes if $q \geq 49$, algebraic geometry codes

  M. A. Tsfasman, S.G. Vladuts, T. Zink, "Modular curves, Shimura curves and Goppa codes, better than Varshamov-Gilbert bound", *Math. Nachrichten*, vol.104, pp.13-28, 1982.

- For $q = 2$, no code C with $\delta_H(C) > \delta$ and rate $R(C) > \mathrm{GV}_q(\delta)$ is reported

GV-Bound: Beyond GV-bound

- Codes of relative distance $> \delta$ and rate r beyond GV-bound ?
  Famous work: Yes if $q \geq 49$, algebraic geometry codes

  M. A. Tsfasman, S.G. Vladuts, T. Zink, "Modular curves, Shimura curves and Goppa codes, better than Varshamov-Gilbert bound", *Math. Nachrichten*, vol.104, pp.13-28, 1982.

- For $q = 2$, no code C with $\delta_H(C) > \delta$ and rate $R(C) > \mathrm{GV}_q(\delta)$ is reported

- A guess: no code of rel. dist. $> \delta$ and rate $> \mathrm{GV}_q(\delta)$ for $q = 2$

GV-Bound: Arbitrary random codes

F: an alphabet
C: random code of rate r of F^n (selected uniformly at random from F^n)

GV-Bound: Arbitrary random codes

F: an alphabet
C: random code of rate r of F^n (selected uniformly at random from F^n)

$$\lim_{n\to\infty} \Pr(\delta_H(C) > \delta) = 1\,, \qquad \text{if} \;\; r < \frac{1}{2}\mathrm{GV}_q(\delta)$$

GV-Bound: Arbitrary random codes

F: an alphabet
C: random code of rate r of F^n (selected uniformly at random from F^n)

$$\lim_{n\to\infty} \Pr(\delta_H(C) > \delta) = 1\,, \qquad \text{if} \quad r < \frac{1}{2}\mathrm{GV}_q(\delta)$$

It follows from:

Alexander Barg, G. David Forney, “Random codes: Minimum distances and error exponents”, *IEEE Trans. Inform. Theory*, vol.48, pp.2568-2573, 2002.

Phase Transitions of Random Codes: What we do ? ?

- F: finite field
  L: random linear code of rate r of F^n

$$\lim_{n\to\infty} \Pr(\delta_H(L) > \delta) = \begin{cases} 1\,, & \text{if } r < \mathrm{GV}_q(\delta)\,; \\ ?\,?\,, & \text{if } r > \mathrm{GV}_q(\delta)\,. \end{cases}$$

Phase Transitions of Random Codes: What we do ? ?

- F: finite field
  L: random linear code of rate r of F^n

$$\lim_{n\to\infty} \Pr(\delta_H(L) > \delta) = \begin{cases} 1\,, & \text{if } r < \mathrm{GV}_q(\delta)\,; \\ ?\,?\,, & \text{if } r > \mathrm{GV}_q(\delta)\,. \end{cases}$$

- F: alphabet
  C: random code of rate r of F^n

$$\lim_{n\to\infty} \Pr(\delta_H(C) > \delta) = \begin{cases} 1\,, & \text{if } r < \frac{1}{2}\mathrm{GV}_q(\delta)\,; \\ ?\,?\,, & \text{if } r > \frac{1}{2}\mathrm{GV}_q(\delta)\,. \end{cases}$$

Phase Transitions of Random Codes: Linear case

F: finite field

L: random linear code of rate r of F^n

Our Result

$$\lim_{n\to\infty} \Pr(\delta_H(L) > \delta) = \begin{cases} 1\,, & \text{if } r < \mathrm{GV}_q(\delta)\,; \\ \mathbf{0}\,, & \text{if } r > \mathrm{GV}_q(\delta)\,. \end{cases}$$

Phase Transitions of Random Codes: Linear case

F: finite field

L: random linear code of rate r of F^n

Our Result

$$\lim_{n\to\infty} \Pr(\delta_H(L) > \delta) = \begin{cases} 1\,, & \text{if } r < \mathrm{GV}_q(\delta)\,; \\ \mathbf{0}\,, & \text{if } r > \mathrm{GV}_q(\delta)\,. \end{cases}$$

Is $\delta_H(L) > \delta$?

$$\text{YES} \; \underset{\substack{r \text{ decreasing} \\ \mathrm{GV}_q(\delta)}}{\overset{\substack{\mathrm{GV}_q(\delta) \\ r \text{ increasing}}}{\rightleftarrows}} \; \text{NO}$$

Linea case: Sketch of proof

Linea case: Sketch of proof

- Random linear map $g : F^k \longrightarrow F^n$

Linea case: Sketch of proof

- Random linear map $g : F^k \longrightarrow F^n$
- Random variables $X_{\mathbf{b}} = \begin{cases} 1, & w_H\big(g(\mathbf{b})\big) \le \delta n; \\ 0, & \text{otherwise.} \end{cases} \quad \mathbf{b} \in F^k.$

Linea case: Sketch of proof

- Random linear map $g : F^k \to F^n$
- Random variables $X_{\mathbf{b}} = \begin{cases} 1, & w_H\big(g(\mathbf{b})\big) \le \delta n; \\ 0, & \text{otherwise.} \end{cases}$ $\mathbf{b} \in F^k$.
- Random variable $X = \sum_{\mathbf{0} \neq \mathbf{b} \in F^k} X_{\mathbf{b}}$.

Linea case: Sketch of proof

- Random linear map $g : F^k \to F^n$
- Random variables $X_{\mathbf{b}} = \begin{cases} 1, & w_H(g(\mathbf{b})) \le \delta n; \\ 0, & \text{otherwise.} \end{cases}$ $\mathbf{b} \in F^k$.
- Random variable $X = \sum_{\mathbf{0} \neq \mathbf{b} \in F^k} X_{\mathbf{b}}$.
- Expectation $\mathrm{E}(X_{\mathbf{b}}) = V_q(n, \delta n)/q^n = V_q(n, \delta n)/q^n \approx q^{-\mathrm{GV}_q(\delta)n}$

Linea case: Sketch of proof

- Random linear map $g : F^k \to F^n$
- Random variables $X_{\mathbf{b}} = \begin{cases} 1, & w_H(g(\mathbf{b})) \le \delta n; \\ 0, & \text{otherwise.} \end{cases} \quad \mathbf{b} \in F^k.$
- Random variable $X = \sum_{\mathbf{0} \neq \mathbf{b} \in F^k} X_{\mathbf{b}}$.
- Expectation $\mathrm{E}(X_{\mathbf{b}}) = V_q(n, \delta n)/q^n = V_q(n, \delta n)/q^n \approx q^{-\mathrm{GV}_q(\delta)n}$
- Expectation $\mathrm{E}(X) = (q^k - 1)\mathrm{E}(X_{\mathbf{b}}) \longrightarrow \begin{cases} 0, & r < \mathrm{GV}_q(\delta); \\ \infty, & r > \mathrm{GV}_q(\delta). \end{cases}$

Linea case: Sketch of proof: Case $r < \mathrm{GV}_q(\delta)$

Case $r < \mathrm{GV}_q(\delta)$

Linea case: Sketch of proof: Case $r < \mathrm{GV}_q(\delta)$

Case $r < \mathrm{GV}_q(\delta)$

By Markov's inequality,

$$\lim_{n\to\infty} \Pr(X \geq 1) \leq \lim_{n\to\infty} \mathrm{E}(X) = 0$$

Linea case: Sketch of proof: Case $r < \mathrm{GV}_q(\delta)$

Case $r < \mathrm{GV}_q(\delta)$

By Markov's inequality,

$$\lim_{n\to\infty} \Pr(X \geq 1) \leq \lim_{n\to\infty} \mathrm{E}(X) = 0$$

so

$$\lim_{n\to\infty} \Pr\left(\delta_H(L) > \delta\right) = \lim_{n\to\infty} \Pr(X = 0) = 1$$

Linea case: Sketch of proof: Case $r > \mathrm{GV}_q(\delta)$

Case $r > \mathrm{GV}_q(\delta)$

Second moment method:

$$\mathsf{Pr}(X \geq 1) \quad \geq \quad \sum_{\mathbf{0} \neq \mathbf{b} \in F^k} \frac{\mathrm{E}(X_{\mathbf{b}})}{\mathrm{E}(X | X_{\mathbf{b}} = 1)}$$

Linea case: Sketch of proof: Case $r > \mathrm{GV}_q(\delta)$

Case $r > \mathrm{GV}_q(\delta)$

Second moment method:

$$\Pr(X \geq 1) \quad \geq \sum_{\mathbf{0} \neq \mathbf{b} \in F^k} \frac{\mathrm{E}(X_{\mathbf{b}})}{\mathrm{E}(X | X_{\mathbf{b}} = 1)}$$

we can compute that

$$\mathrm{E}(X | X_{\mathbf{b}} = 1) = (q^k - q)\mathrm{E}(X_{\mathbf{b}}) + (q - 1)$$

Linea case: Sketch of proof: Case $r > \mathrm{GV}_q(\delta)$

Case $r > \mathrm{GV}_q(\delta)$

Second moment method:

$$\Pr(X \geq 1) \quad \geq \quad \sum_{\mathbf{0} \neq \mathbf{b} \in F^k} \frac{\mathrm{E}(X_{\mathbf{b}})}{\mathrm{E}(X | X_{\mathbf{b}} = 1)}$$

we can compute that

$$\mathrm{E}(X | X_{\mathbf{b}} = 1) = (q^k - q)\mathrm{E}(X_{\mathbf{b}}) + (q - 1)$$

from that $\lim_{n \to \infty} q^k \mathrm{E}(X_{\mathbf{b}}) = \lim_{n \to \infty} \mathrm{E}(X) = \infty$, we have

$$\lim_{n \to \infty} \Pr(X \geq 1) \geq \lim_{n \to \infty} \frac{q^k \mathrm{E}(X_{\mathbf{b}})}{(q^k - q)\mathrm{E}(X_{\mathbf{b}}) + (q - 1)} = 1$$

Linea case: Sketch of proof: Case $r > \mathrm{GV}_q(\delta)$

Case $r > \mathrm{GV}_q(\delta)$

Second moment method:

$$\Pr(X \geq 1) \quad \geq \quad \sum_{\mathbf{0} \neq \mathbf{b} \in F^k} \frac{\mathrm{E}(X_{\mathbf{b}})}{\mathrm{E}(X | X_{\mathbf{b}} = 1)}$$

we can compute that

$$\mathrm{E}(X | X_{\mathbf{b}} = 1) = (q^k - q)\mathrm{E}(X_{\mathbf{b}}) + (q - 1)$$

from that $\lim_{n \to \infty} q^k \mathrm{E}(X_{\mathbf{b}}) = \lim_{n \to \infty} \mathrm{E}(X) = \infty$, we have

$$\lim_{n \to \infty} \Pr(X \geq 1) \geq \lim_{n \to \infty} \frac{q^k \mathrm{E}(X_{\mathbf{b}})}{(q^k - q)\mathrm{E}(X_{\mathbf{b}}) + (q - 1)} = 1$$

so

$$\lim_{n \to \infty} \Pr\left(\delta_H(L) > \delta\right) = \lim_{n \to \infty} \Pr(X = 0) = 0$$

Phase transitions of Random Codes: Arbitrary case

F: an alphabet

C: random code of rate r of F^n

Our Result

$$\lim_{n\to\infty} \Pr(\delta_H(C) > \delta) = \begin{cases} 1, & \text{if } r < \frac{1}{2}\mathrm{GV}_q(\delta); \\ \mathbf{0}, & \text{if } r > \frac{1}{2}\mathrm{GV}_q(\delta). \end{cases}$$

Phase transitions of Random Codes: Arbitrary case

F: an alphabet

C: random code of rate r of F^n

Our Result

$$\lim_{n\to\infty} \mathrm{Pr}(\delta_H(C) > \delta) = \begin{cases} 1\,, & \text{if } \ r < \frac{1}{2}\mathrm{GV}_q(\delta)\,; \\ \mathbf{0}\,, & \text{if } \ r > \frac{1}{2}\mathrm{GV}_q(\delta)\,. \end{cases}$$

Is $\delta_H(C) > \delta$?

$$\text{YES} \ \underset{\substack{r \text{ decreasing} \\ \frac{1}{2}\mathrm{GV}_q(\delta)}}{\overset{\substack{\frac{1}{2}\mathrm{GV}_q(\delta) \\ r \text{ increasing}}}{\rightleftarrows}} \ \text{NO}$$

Pictures for Phase Transitions: Linear case

Linear case: random linear code L

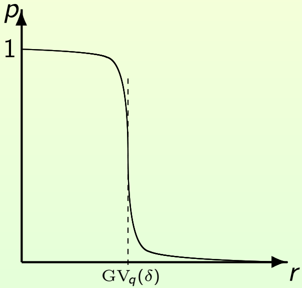


Figure: $p = \Pr\left(\delta_H(L) > \delta\right)$; $0 < \delta < \delta_0$.

Pictures for Phase Transitions: Linear case

Linear case: random linear code L

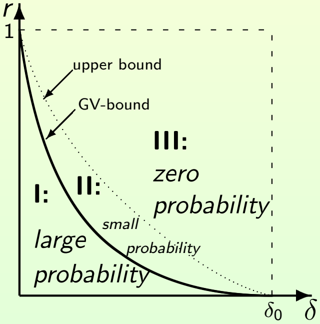
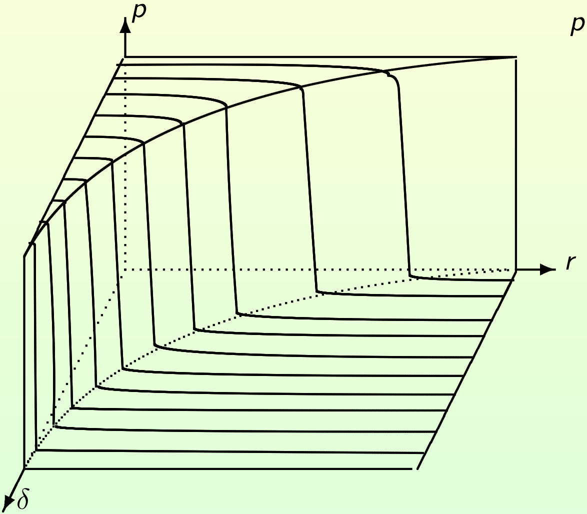


Figure: Three areas for the probability of the event "$\delta_H(L) > \delta$"

Pictures for Phase Transitions: Linear case

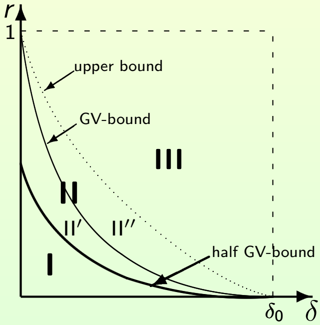


$p = \Pr(\delta_H(L) > \delta)$

$r = \mathrm{GV}_q(\delta)$ is a phase transition curve

Pictures for Phase Transitions: Arbitrary case

Arbitrary case: arbitrary random code C



I: probability ~ 1

II: probability ~ 0

II': greedy algorithm works

II": greedy algorithm does't work

III: probability $= 0$

Figure: Three (four) areas for the probability of the event "$\delta_H(C) > \delta$"

THANK YOU