Asymptotically good codes

Stefan van Zwam

Department of Mathematics
Louisiana State University

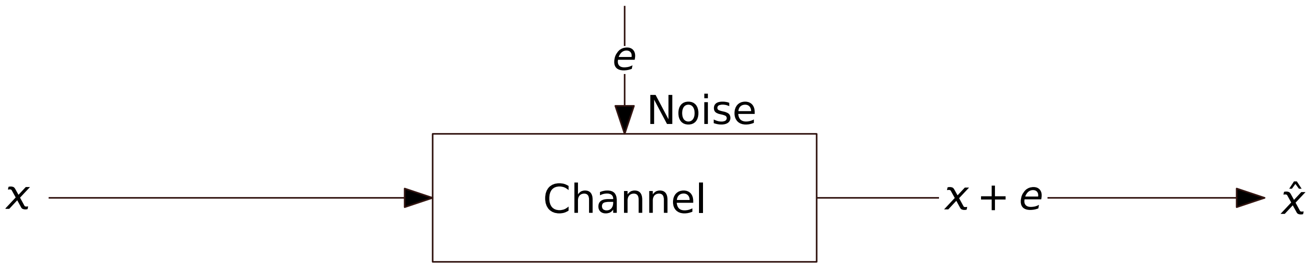
Based on joint work with Peter Nelson

Geoff Whittle's 65$^{\text{th}}$ birthday conference
Wellington, New Zealand, December 2015

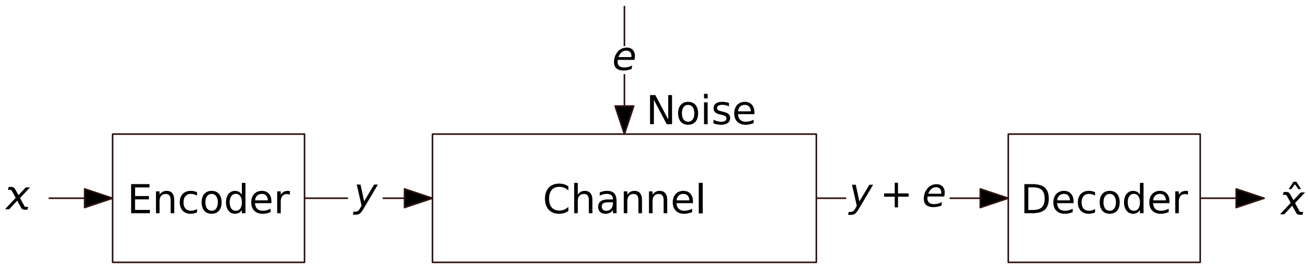
Contents

Part I
Error-correcting codes

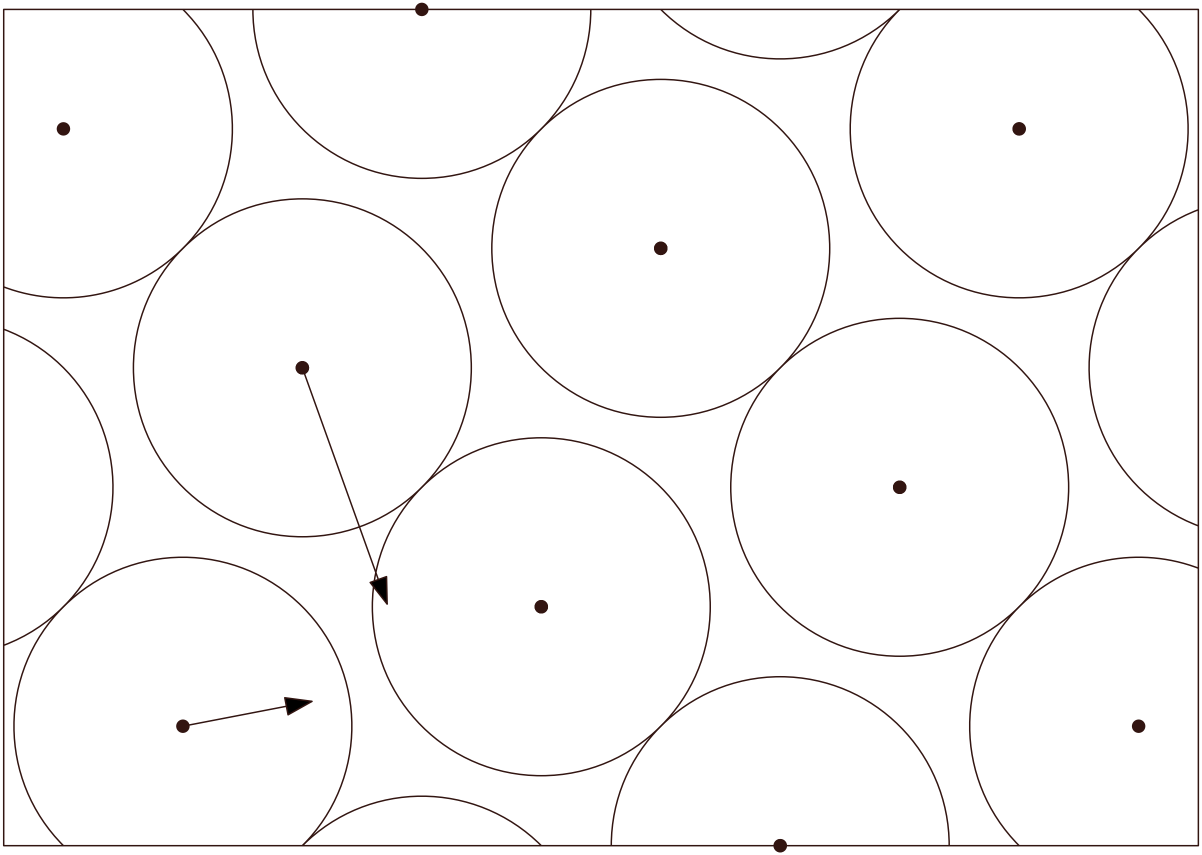
Error-correcting codes



Error-correcting codes



Error-correcting codes



Error-correcting codes

- Code C is subset of $\mathrm{GF}(2)^n$.
- Error model: each bit flipped with small probability p.
- *Distance:* $d(x, y) := |\{i : x_i \neq y_i\}|$.

Linear codes

- Code C is k-dimensional sub*space* of $\mathrm{GF}(2)^n$.
- Notation: $[n, k, d]$ linear code.

$$d = \min_{x,y \in C} d(x, y)$$

Linear codes

- Code C is k-dimensional sub*space* of $GF(2)^n$.
- Notation: $[n, k, d]$ linear code.

$$\begin{aligned} d &= \min_{x,y \in C} d(x, y) \\ &= \min_{x,y \in C} |\{i : x_i \neq y_i\}| \end{aligned}$$

Linear codes

- Code C is k-dimensional sub*space* of $\mathrm{GF}(2)^n$.
- Notation: $[n, k, d]$ linear code.

$$\begin{aligned} d &= \min_{x,y\in C} d(x,y) \\ &= \min_{x,y\in C} |\{i : x_i \neq y_i\}| \\ &= \min_{x,y\in C} |\{i : x_i - y_i \neq 0\}| \end{aligned}$$

Linear codes

- Code C is k-dimensional sub*space* of $\mathrm{GF}(2)^n$.
- Notation: $[n,k,d]$ linear code.

$$\begin{aligned} d &= \min_{x,y\in C} d(x,y) \\ &= \min_{x,y\in C} |\{i : x_i \neq y_i\}| \\ &= \min_{x,y\in C} |\{i : x_i - y_i \neq 0\}| \\ &= \min_{z\in C} |\{i : z_i \neq 0\}| \end{aligned}$$

Linear codes

- Code C is k-dimensional sub*space* of $\mathrm{GF}(2)^n$.
- Notation: $[n, k, d]$ linear code.

$$
\begin{aligned}
d &= \min_{x,y\in C} d(x,y) \\
&= \min_{x,y\in C} |\{i : x_i \neq y_i\}| \\
&= \min_{x,y\in C} |\{i : x_i - y_i \neq 0\}| \\
&= \min_{z\in C} |\{i : z_i \neq 0\}| \\
&= \min_{z\in C} d(z,0)
\end{aligned}
$$

Asymptotically good codes

- Family $C_1, C_2, \ldots$ of linear codes with parameters $[n_i, k_i, d_i]$ is *asymptotically good* if, for some $\varepsilon > 0$:

(*i*) *Growing size:* $n_i \to \infty$ as $i \to \infty$

(*ii*) *Constant rate:* $k_i/n_i \geq \varepsilon$

(*iii*) *Growing minimum distance:* $d_i/n_i \geq \varepsilon$

Asymptotically good codes

- Family $C_1, C_2, \ldots$ of linear codes with parameters $[n_i, k_i, d_i]$ is *asymptotically good* if, for some $\varepsilon > 0$:

(*i*) *Growing size:* $n_i \to \infty$ as $i \to \infty$

(*ii*) *Constant rate:* $k_i/n_i \geq \varepsilon$

(*iii*) *Growing minimum distance:* $d_i/n_i \geq \varepsilon$

Theorem. Asymptotically good codes exist.

- Random codes
- Constructions using expanders (e.g. Alon, Bruck, Naor, Naor, Roth)
- Goppa codes, Justensen Codes

Asymptotically good codes: structure?

Operations on a code:

- **Puncturing:** $C \backslash i$, remove ith coordinate from each word
- **Shortening:** C/i, take $\{c \in C : c_i = 0\}$, then remove ith coordinate.

Asymptotically good codes: structure?

Operations on a code:

- **Puncturing:** $C \setminus i$, remove ith coordinate from each word
- **Shortening:** C/i, take $\{c \in C : c_i = 0\}$, then remove ith coordinate.

Theorem (Nelson, vZ 2015). Let $\mathcal{M}$ be a class of binary linear codes closed under puncturing, shortening. If $\mathcal{M}$ contains an asymptotically good sequence, then $\mathcal{M}$ contains *all* codes.

Part II
Matroids and minors

Matroids

Let $\mathcal{C}^*$ be the codewords in C with inclusionwise minimal *support*.

Matroids

Let $\mathcal{C}^*$ be the codewords in C with inclusionwise minimal *support*.

Theorem. $\mathcal{C}^*$ is the set of cocircuits of a matroid $M(C)$.

Matroids

Let $\mathcal{C}^*$ be the codewords in C with inclusionwise minimal *support*.

Theorem. $\mathcal{C}^*$ is the set of cocircuits of a matroid $M(C)$.

Theorem. $M(C\backslash i) = M(C)\backslash i$ and $M(C/i) = M(C)/i$.

Matroids

Let $\mathcal{C}^*$ be the codewords in C with inclusionwise minimal *support*.

Theorem. $\mathcal{C}^*$ is the set of cocircuits of a matroid $M(C)$.

Theorem. $M(C\backslash i) = M(C)\backslash i$ and $M(C/i) = M(C)/i$.

Def. *Dual* code $C^{\perp}$ is orthogonal complement of subspace C.

Theorem. $M(C^{\perp}) = M(C)^*$.

Matroids

Let $\mathcal{C}^*$ be the codewords in C with inclusionwise minimal *support*.

Theorem. $\mathcal{C}^*$ is the set of cocircuits of a matroid $M(C)$.

Theorem. $M(C\backslash i) = M(C)\backslash i$ and $M(C/i) = M(C)/i$.

Def. *Dual* code $C^\perp$ is orthogonal complement of subspace C.

Theorem. $M(C^\perp) = M(C)^*$.

Theorem. Put basis of C as rows of A. Then $C = \text{rowspace}(A)$ and $M(C) = M[A]$.

(Co)graphic matroids

Code C is *graphic* if C is cycle space of graph G. So $M(C)$ is *cographic* matroid.

Theorem (Kashyap 2008). The family of duals of graphic codes is not asymptotically good.

(Co)graphic matroids

Code C is *graphic* if C is cycle space of graph G. So $M(C)$ is *cographic* matroid.

Theorem (Kashyap 2008). The family of duals of graphic codes is not asymptotically good.

Theorem (Kashyap 2008). The family of graphic codes is not asymptotically good.

(Co)graphic matroids

Code C is *graphic* if C is cycle space of graph G. So $M(C)$ is *cographic* matroid.

Theorem (Kashyap 2008). The family of duals of graphic codes is not asymptotically good.

Theorem (Kashyap 2008). The family of graphic codes is not asymptotically good.

Proof sketch: Hinges on (Alon, Hoory, Linial): if G has average degree $\delta > 2$, then $\mathrm{girth}(G) \leq \log(|V(G)| - \delta + 1)$.

Part III
Matroid Structure Theory

The Structure of Highly Connected Matroids

Geelen, Gerards, Whittle announced proof of the following:

Theorem. Let $\mathcal{M}$ be proper minor-closed class of binary matroids. There exist k, t such that every vertically k-connected matroid $M \in \mathcal{M}$ has M or M^* equal to a rank-t perturbation of a graphic matroid.

The Structure of Highly Connected Matroids

Geelen, Gerards, Whittle announced proof of the following:

Theorem. Let $\mathcal{M}$ be proper minor-closed class of binary matroids. There exist k, t such that every vertically k-connected matroid $M \in \mathcal{M}$ has M or M^* equal to a rank-t perturbation of a graphic matroid.

Perturbation: add low-rank matrix to representation. Matroidal view: small number of *lifts* and *projections*.

Applying the theorem

Two steps to prove our result:

- If asymptotically good family exists, may assume members are highly connected
- Low-rank perturbations don't break Kashyap's re-sults

Connectivity

An (α, β)-*good sequence* in $\mathcal{M}$:

- $n_i \geq i$
- $k_i/n_i \geq \alpha$
- $d_i/n_i \geq \beta$

Choose (α, β) “optimal”; take a sufficiently large M_i with low-order separation. Show: can trade off some α for better β. Hence, this happens finitely often.

Keeping a short circuit

Key observation:

Lemma. If M_2 is a rank-t perturbation of M_1, then

$$|r_{M_2}(X) - r_{M_1}(X)| \leq 2t$$

Repeat Alon-Hoory-Linial to get $2t+1$ log-size circuits in M_1. Take their union X. Then $r_{M_2}(X) < |X|$.

Generalization

Theorem (Nelson, vZ). If $\mathcal{M}$ proper subclass of GF(p^n)-representable matroids, not containing all GF(p)-representable matroids, then $\mathcal{M}$ has no asymptotically good sequence.

Generalization

Theorem (Nelson, vZ). If $\mathcal{M}$ proper subclass of GF(p^n)-representable matroids, not containing all GF(p)-representable matroids, then $\mathcal{M}$ has no asymptotically good sequence.

Future

Maximum-Likelihood Threshold. For fixed rate R, which channel errors p allow arbitrarily good communication with a code from $\mathcal{M}$?

- Cographic: 0
- Graphic: $\frac{(1-\sqrt{R})^2}{2(1+R)}$
  (Decreusefond, Zémor: regular graphs; Nelson, vZ: arbitrary graphs)
- Minor-closed: TODO

Slides, preprints at

http://www.math.lsu.edu/~svanzwam/

The End