

Coverings and packings for radius 1 adaptive block coding

Robert B. Ellis

Illinois Institute of Technology

DIMACS/DIMATIA/Rényi Inst. Combinatorial Challenges 2006

Outline

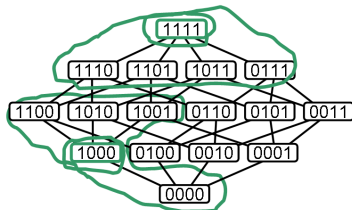
- 1 Background
 - Non-adaptive and adaptive radius 1 codes
 - Liar games
 - Previous work
- 2 New Contribution
 - Constructive bottom-up algorithm
 - Ingredients of the proof
 - Exact sizes of optimal codes
- 3 Open questions and concluding remarks

1-balls & non-adaptive radius 1 block codes defined

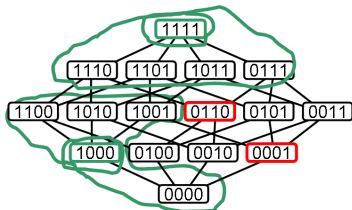
- **Hypercube** $Q_{n,t} := \{x_1 \cdots x_n \in \{0, \dots, t-1\}^t\}$
- **Hamming distance** $d(x, y) = |\{i : x_i \neq y_i\}|$
- **1-ball** $B_1(u) := \{u \in Q_{n,t} : d(u, v) \leq 1\}$
- **1-ball size** $b_1(n, t) := 1 + n(t-1)$

1111
 0111
 1011
 1101
 1110

$B_1(1111)$



Packing code in $Q_{4,2}$



Covering code in $Q_{4,2}$

Optimal radius 1 block codes defined

- $F_t(n, 1) :=$ maximum size of packing of 1-balls in $Q_{n,t}$
- $K_t(n, 1) :=$ minimum size of covering of 1-balls in $Q_{n,t}$
- **Sphere bound.** $F_t(n, 1) \leq \frac{t^n}{1+n(t-1)} \leq K_t(n, 1)$

For $t = 2$:

- **Hamming codes.** $(n + 1) | 2^n \Rightarrow F_2(n, 1) = K_2(n, 1)$
- **Asymptotics (Kabatyanskii and Panchenko).** $\lim_{n \rightarrow \infty} \frac{F_t(n, 1)}{K_t(n, 1)} = 1$

1-sets & radius 1 adaptive block codes defined

- a **1-set** consists of

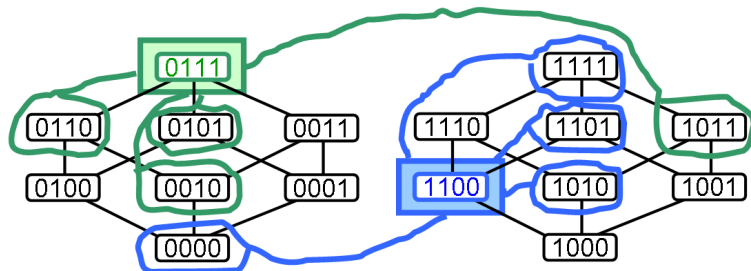
$$\begin{array}{ll} \text{a stem} & x_1 \cdots x_{i-1} x_i \cdots x_n \in Q_{n,t} \\ n(t-1) \text{ children} & x_1 \cdots x_{i-1} y_i * \cdots * \in x_1 \cdots x_i y_i Q_{n-i,t}, \end{array}$$

where $y_i \in [t] \setminus x_i$.

- Examples.

$$\begin{array}{ll} & 2021 \\ & \underline{0000} \\ & \underline{1100} \\ & \underline{0010} \\ n = 4, t = 2: & \underline{1001} \\ & \underline{1111} \\ & \underline{1101} \\ & 2021 \\ & \underline{0000} \\ & \underline{1102} \\ & \underline{2121} \\ n = 4, t = 3: & \underline{2200} \\ & \underline{2002} \\ & \underline{2011} \\ & \underline{2020} \\ & \underline{2022} \end{array}$$

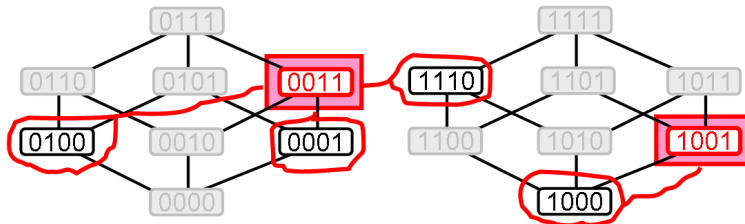
Example radius 1 adaptive packing



Adaptive packing code in $Q_{4,2}$

0111	1100
<u>1</u> 011	<u>0</u> 000
00 <u>1</u> 0	1 <u>0</u> 11
01 <u>0</u> 1	11 <u>0</u> 1
011 <u>0</u>	110 <u>1</u>

Example radius 1 adaptive covering



Adaptive covering code in $Q_{4,2}$

Previous packing, plus:

0011	1001	
<u>1</u> 110	signature = 5, 5, 4, 2
0 <u>1</u> 00	
00 <u>0</u> 1	
....	<u>1</u> 000	

Optimal radius 1 adaptive block codes defined

- $F'_t(n, 1) :=$ maximum size of packing of 1-sets in $Q_{n,t}$
- $K'_t(n, 1) :=$ minimum size of covering of 1-sets in $Q_{n,t}$

- **Sphere bound⁺.**

$$F_t(n, 1) \leq F'_t(n, 1) \leq \frac{t^n}{1+n(t-1)} \leq K'_t(n, 1) \leq K_t(n, 1)$$

Optimal radius 1 adaptive block codes defined

- $F'_t(n, 1) :=$ maximum size of packing of 1-sets in $Q_{n,t}$
- $K'_t(n, 1) :=$ minimum size of covering of 1-sets in $Q_{n,t}$

- **Sphere bound⁺.**

$$F_t(n, 1) \leq F'_t(n, 1) \leq \frac{t^n}{1+n(t-1)} \leq K'_t(n, 1) \leq K_t(n, 1)$$

- **Binary case** (EIS, CHLL; P, EPY)

n	1	2	3	4	5	6	7	8	9	10	11
$F_2(n, 1)$	1	1	2	2	4	8	16	20	40	72	144
$F'_2(n, 1)$	1	1	2	2	4	8	16	28	50	92	170
$K'_2(n, 1)$	1	2	2	4	6	10	16	30	52	94	172
$K_2(n, 1)$	1	2	2	4	7	12	16	32	≤ 57	≤ 105	≤ 180

Liar games defined

2-player perfect information game

- **Players:** **Paul** – partitioner/questioner
Carole – chooser/responder
- q rounds of **Game play:**
Paul partitions $[n] \rightarrow A_1 \dot{\cup} \dots \dot{\cup} A_t$
Carole selects a part, other parts get 1 lie
Elements with $\leq k$ lies **survive**

Possible winning conditions for Paul

- **Original.** ≤ 1 element survives (Rényi, Ulam)
- **Pathological.** ≥ 1 element survives (Ellis+Yan)

Equivalence of liar games and packings/coverings

- **Offline** partitions by **Paul**
 - Winning strategy in **original game** \leftrightarrow **nonadaptive packing** in hypercube
 - Winning strategy in **pathological game** \leftrightarrow **nonadaptive covering** in hypercube

Equivalence of liar games and packings/coverings

- **Offline** partitions by Paul
 - Winning strategy in **original game** \leftrightarrow **nonadaptive packing** in hypercube
 - Winning strategy in **pathological game** \leftrightarrow **nonadaptive covering** in hypercube
- **Online** partitions by Paul
 - Winning strategy in **original game** \leftrightarrow **adaptive packing** in hypercube
 - Winning strategy in **pathological game** \leftrightarrow **adaptive covering** in hypercube

Equivalence of liar games and packings/coverings

- **Offline** partitions by Paul
 - Winning strategy in **original game** \leftrightarrow **nonadaptive packing** in hypercube
 - Winning strategy in **pathological game** \leftrightarrow **nonadaptive covering** in hypercube
- **Online** partitions by Paul
 - Winning strategy in **original game** \leftrightarrow **adaptive packing** in hypercube
 - Winning strategy in **pathological game** \leftrightarrow **adaptive covering** in hypercube

Remarks. Parameters n, t, k must match!

Many generalizations:

attributions $\subseteq 2^{\{\text{Spencer, Yan, Dumitriu, Ellis, Ponomarenko, Nyman}\}}$

Sample of previous bounds on adaptive codes

Adaptive packing codes/liar games

- (Berlekamp '67) Fixed k , weight function
- (Spencer+Winkler '91) $k \sim q/3, q/4$ (balls off a cliff...)
- (Spencer '92) $F'_2(n, k) \pm C_k$ for fixed k
- (Pelc, Guzicki, Deppe) exact $F'_2(n, k)$ for $k = 1, 2, 3$, resp.
- (Cicalese+Mundici, Spencer \oplus {Dumitriu, Yan}) half-lie: $k = 1$ and fixed k , resp.
- (Spencer+Dumitriu, Ellis+Nyman) fixed k ; arbitrary channel, arbitrary channels, resp.

Adaptive covering codes/pathological liar games

- (Ellis+Yan, Ellis+Ponomarenko+Yan) half-lie for $k = 1$, $K'_2(n, k) \pm C_k$ for fixed k

Example collaboration.



Example collaboration.



S. “The $\{x_2, x_1 x_3\}$ partitioning is clearly best.”

Example collaboration.



- S. “The $\{x_2, x_1 x_3\}$ partitioning is clearly best.”
- Ł. “Who are you playing for, Paul or Carole?”

Example collaboration.



- S. “The $\{x_2, x_1 x_3\}$ partitioning is clearly best.”
- Ł. “Who are you playing for, Paul or Carole?”
- S. “I don’t remember, but the answer is $1/3$.”

Philosophy of approach

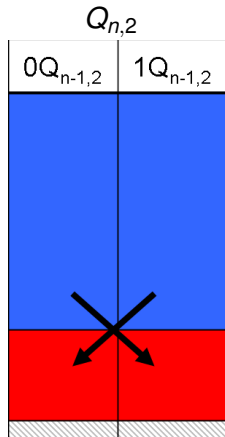
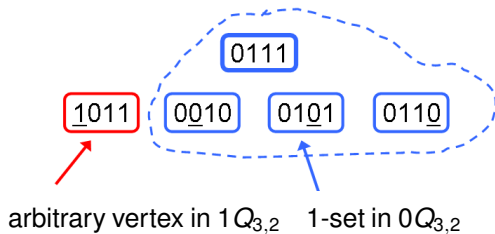
Previously, 4 proofs for any choice of k , t , channel

- Upper (sphere) bound for adaptive packing
- Exhibition of good adaptive packing
- Lower (sphere) bound for adaptive covering
- Exhibition of good adaptive covering

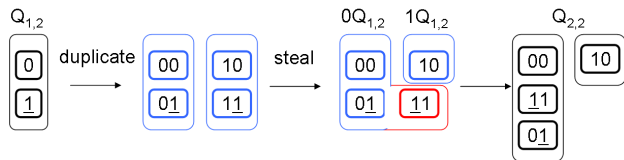
Goal: single unified proof (& fast algorithm)

Decomposition structure of 1-sets in $Q_{n,2}$

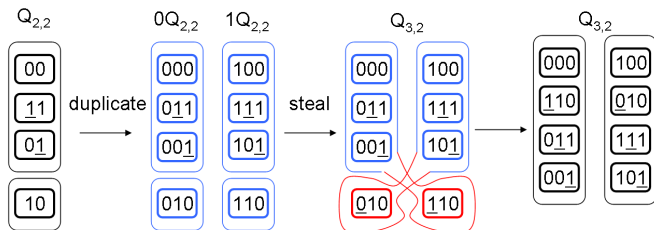
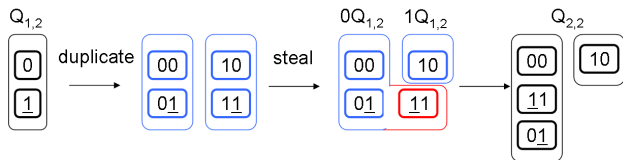
Observation. $t = 2$



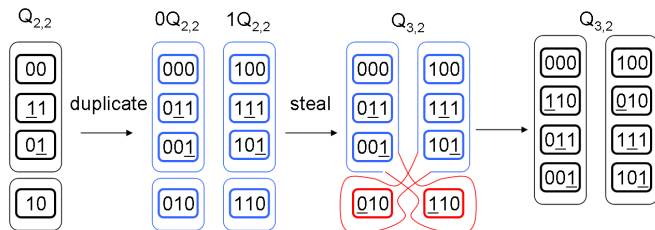
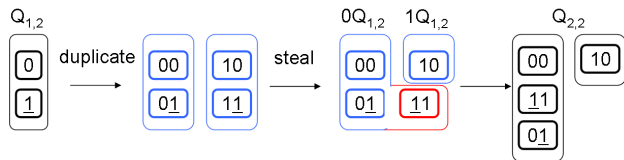
Packing within covering **duplication** algorithm



Packing within covering **duplication** algorithm



Packing within covering **duplication** algorithm



Signature encoding of $Q_{2,2} \rightarrow Q_{3,2}$

$$\begin{array}{c}
 Q_{2,2} \\
 \hline
 3 \\
 1
 \end{array}
 \xrightarrow{\text{dup.}}
 \begin{array}{cc}
 0Q_{2,2} & 1Q_{2,2} \\
 \hline
 3 & 3 \\
 1 & 1
 \end{array}
 \xrightarrow{\text{st.}}
 \begin{array}{cc}
 0Q_{2,2} & 1Q_{2,2} \\
 \hline
 4 & 4
 \end{array}
 \leftrightarrow
 \begin{array}{c}
 Q_{3,2} \\
 \hline
 4 \\
 4
 \end{array}$$

Dominant signature of a collection of 1-sets defined

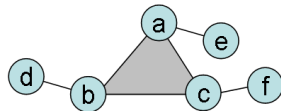
Definition

A **dominant signature** of a collection \mathcal{F} of m 1-sets is an ordering F_1, \dots, F_m and a sequence $\alpha_1, \dots, \alpha_m$ such that for all J ,

$$|F_1 \cup F_2 \cup \dots \cup F_J| = \alpha_1 + \alpha_2 + \dots + \alpha_J,$$

and for each J , no J -subset of \mathcal{F} is larger than $\sum_{i=1}^J \alpha_i$.

Remark. Always monotonic decreasing, but doesn't always exist:



3, 4, **5**, 6 (triangle first)

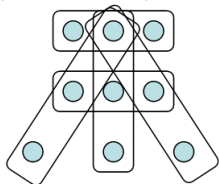
2, 4, **6**, 6 (triangle last)

$\{abc, ae, bd, cf\}$

Dominant signature of a collection of 1-sets defined

More counterexamples.

(Vera Asodi) Minimum ground set 3-uniform counterexample



(Penny Haxell, Gábor Tardos) Whiteboard

Radius 1 adaptive codes with dominant signatures

Lemma

If the set of all 1-sets \mathcal{F} in $Q_{n,t}$ has a dominant signature $(\alpha(n, t, i))_{i \geq 1}$, then

- **Packing:** $\alpha(n, t, 1) = \dots = \alpha(n, t, F'_t(n, 1)) = 1 + t(n - 1)$,
- **Covering:** $\alpha(n, t, K'_t(n, 1)) > \alpha(n, t, K'_t(n, 1) + 1) = 0$, and
- **Partial covering:** for all J , the most vertices which can be covered by J 1-sets is exactly

$$\alpha(n, t, 1) + \alpha(n, t, 2) + \dots + \alpha(n, t, J) = |F_1 \cup F_2 \cup \dots \cup F_J|.$$

Remark. Dominant signature \Rightarrow optimal packing within optimal covering.

More iterations of the duplication algorithm

$\begin{array}{c} Q_{3,2} \\ 4 \\ 4 \end{array}$	$\xrightarrow{\text{dup.}}$	$\begin{array}{c c} 0Q_{3,2} & 1Q_{3,2} \\ \hline 4 & 4 \\ 4 & 4 \end{array}$	$\xrightarrow{\text{st. (a)}}$	$\begin{array}{c c} 0Q_{3,2} & 1Q_{3,2} \\ \hline 5 & 5 \\ 3 & 3 \end{array}$	$\xrightarrow{\text{st. (b)}}$	$\begin{array}{c c} 0Q_{2,2} & 1Q_{2,2} \\ \hline 5 & 5 \\ 4 & 2 \end{array}$
$\begin{array}{c} Q_{4,2} \\ 5 \\ 5 \\ 4 \\ 2 \end{array}$	$\xrightarrow{\text{dup.}}$	$\begin{array}{c c} 0Q_{4,2} & 1Q_{4,2} \\ \hline 5 & 5 \\ 5 & 5 \\ 4 & 4 \\ 2 & 2 \end{array}$	$\xrightarrow{\text{st. (a)}}$	$\begin{array}{c c} 0Q_{4,2} & 1Q_{4,2} \\ \hline 6 & 6 \\ 6 & 6 \\ 4 & 4 \end{array}$	$\xrightarrow{\text{st. (b)}}$	$\begin{array}{c c} 0Q_{4,2} & 1Q_{4,2} \\ \hline 6 & 6 \\ 6 & 6 \\ 5 & 3 \end{array}$
$\begin{array}{c} Q_{5,2} \\ 6 \\ 6 \\ 6 \\ 6 \\ 5 \\ 3 \end{array}$	$\xrightarrow{\text{dup.}}$	$\begin{array}{c c} 0Q_{5,2} & 1Q_{5,2} \\ \hline 6 & 6 \\ 6 & 6 \\ 6 & 6 \\ 6 & 6 \\ 5 & 5 \\ 3 & 3 \end{array}$	$\xrightarrow{\text{st. (a)}}$	$\begin{array}{c c} 0Q_{5,2} & 1Q_{5,2} \\ \hline 7 & 7 \\ 7 & 7 \\ 7 & 7 \\ 7 & 7 \\ 4 & 4 \end{array}$	$\xrightarrow{\text{st. (b)}}$	$\begin{array}{c c} 0Q_{5,2} & 1Q_{5,2} \\ \hline 7 & 7 \\ 7 & 7 \\ 7 & 7 \\ 7 & 7 \\ 5 & 3 \end{array}$

Domination preserved by duplication algorithm

Lemma (Domination lemma)

If the input signature for the duplication algorithm is dominant for $Q_{n,t}$, then the output signature is dominant for $Q_{n+1,t}$.

Remark. i.e., optimal packing within covering for $n \Rightarrow$
optimal packing within covering for $n + 1$

Lemma (Covering lemma)

Let $(\alpha(n, t, i))_{i=1}^M$ be a dominant signature for $Q_{n,t}$, and $\sum_{i=0}^{t-1} M_i = M$. Then the most vertices of $Q_{n+1,t}$ which can be covered by M_i 1-sets with stem in $iQ_{n,t}$ is $C(n+1, t, M_0, \dots, M_{t-1}) :=$

$$\sum_{i=0}^{t-1} \left(\sum_{j=1}^{M_i} \alpha(n, t, j) + \min \left\{ t^n - \sum_{j=1}^{M_i} \alpha(n, t, j), M - M_i \right\} \right).$$

Proving the domination lemma

Proof sketches of the covering and domination lemmas.

- The **inner summation** is concave; therefore $C(n+1, t, M_0, \dots, M_{t-1})$ is maximized when $|M_i - M_j| \leq 1$ for all i, j .

$$\sum_{j=1}^{M_i} \alpha(n, t, j) + \min \left\{ t^n - \sum_{j=1}^{M_i} \alpha(n, t, j), M - M_i \right\}.$$

- Output signature β of duplication has $M_0 \geq \dots \geq M_{t-1} \geq M_0 - 1$.
- Output signature $(\beta(n+1, t, j))_{j \geq 1}$ satisfies for all K (w/abuse),

$$\sum_{j=1}^K \beta(n+1, t, j) = C(n+1, t, \lceil K/t \rceil, \dots, \lfloor K/t \rfloor).$$



Sample case computation for duplication output

Case: • last row which makes a **full steal** is r

- last nonzero β at index $M > t \cdot r$
- give back all stealing done by indices $> t \cdot r$
- $\beta = t^n - \sum_{i=1}^r (\alpha(n, t, i) + t - 1) + t - (M - t \cdot r)$
at indices $t \cdot r + 1, \dots, M$. Then

$$\begin{aligned}
 \sum_{j=1}^M \beta(n+1, t, j) &= \sum_{j=1}^{tr} (\alpha(n, t, \lceil j/t \rceil) + t - 1) \\
 &\quad + (M - tr) \left(t^n - \sum_{j=1}^r (\alpha(n, t, j) + t - 1) + t - M + tr \right) \\
 &= \sum_{i=1}^t \left(\sum_{j=1}^r \alpha(n, t, j) + rt - r \right) + (M - tr)(t - (M - tr)) \\
 &\quad + (M - tr) \left(t^n - \sum_{j=1}^r \alpha(n, t, j) - rt + r \right) \\
 &= \sum_{i=1}^{M-tr} t^n + \sum_{i=M-tr+1}^t \left(\sum_{j=1}^r \alpha(n, t, j) + M - r \right) \\
 &\geq C(n+1, t, \lceil M/t \rceil, \dots, \lceil M/t \rceil, \lfloor M/t \rfloor, \dots, \lfloor M/t \rfloor).
 \end{aligned}$$

Optimal adaptive packing and covering numbers

Theorem

Let $t \geq 2$ and $n \geq t + 1$. There exists an optimal radius 1 adaptive packing contained in an optimal radius 1 adaptive covering of $Q_{n,t}$ with respective sizes $F'_t(n, 1)$, $K'_t(n, 1)$ given by

$t^{n-1} \bmod b_{n,t}(1)$	$F'_t(n, 1)$	$K'_t(n, 1)$
$i, 0 \leq i < t$	tS	$tS + i$
$t, \dots, b_{n-1,t}(1) - 1$	tS	$tS + t$
$b_{n-1,t}(1) - 1 + i, 1 \leq i < t$	$tS + i$	$tS + t$

where $b_{n,t}(1) = 1 + n(t - 1)$ and $S = \lfloor t^{n-1} / b_{n,t}(1) \rfloor$.

Remarks. For $1 \leq n \leq t + 1$:

- $F'_t(n, 1) = t^{n-2}$
- $K'_t(n, 1)$ boundable but complicated

Open questions

Related to this technique:

- For which other communication channels does the **domination lemma** hold for radius 1?
- Can we extend the duplication algorithm to other communication channels, radius > 1 ?

General adaptive coding questions:

- Tight bounds when radius = $\omega(1)$?
- Can known methods improve coin-weighing, batch-testing, or liar games with restricted questions?

And of course, do fixed-radius nonadaptive codes approach the sphere bound?

SIAM Victoria Minisymposium: “Liar games and error-correcting codes”

Organizers: Ioana Dumitriu, Joel Spencer, New York University

- **Berlekamp.** History of Block Coding with Noiseless Feedback
- **Dumitriu+Spencer.** Liar Games with a Fixed Number of Constrained Lies
- **Ahlsvede+Cicalese+Deppe.** Searching with Lies under Error Cost Constraints
- **Ahlsvede+Deppe.** Non-Binary Error-Correcting Codes with Noiseless Feedback
- **Ellis+Nyman.** Multichannel Liar Games with a Fixed Number of Lies

Survey: A. Pelc. Searching games with errors—fifty years of coping with liars, Theoret. Comput. Sci. '02.