Coverings and packings for radius 1 adaptive block coding

Robert B. Ellis
Illinois Institute of Technology

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** \( Q_{n,t} := \{ x_1 \cdots x_n \in \{0, \ldots, t-1\}^n \} \)
- **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** \( b_1(n, t) := 1 + n(t - 1) \)

\[
\begin{array}{c}
1111 \\
0111 \\
1011 \\
1101 \\
1110 \\
B_1(1111)
\end{array}
\]

Packing code in \( Q_{4,2} \)

Covering code in \( Q_{4,2} \)
Optimal radius 1 block codes defined

- $F_t(n, 1) := \text{maximum size of packing of 1-balls in } Q_{n,t}$
- $K_t(n, 1) := \text{minimum size of covering of 1-balls in } Q_{n,t}$
- 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). $\lim_{n \to \infty} \frac{F_2(n,1)}{K_2(n,1)} = 1$
1-sets & radius 1 adaptive block codes defined

- A 1-set consists of
  - A stem: $x_1 \cdots x_{i-1}x_i \cdots x_n \in Q_{n,t}$
  - $n(t - 1)$ children: $x_1 \cdots x_{i-1}y_i* \cdots * \in x_1 \cdots x_i y_i Q_{n-i,t}$, where $y_i \in [t] \setminus x_i$.

- Examples.

$n = 4, t = 2$: $1001$

$n = 4, t = 3$: $1100$

$n = 4, t = 3$: $1102$

$n = 4, t = 3$: $0010$

$n = 4, t = 3$: $2121$

$n = 4, t = 3$: $2000$

$n = 4, t = 3$: $2021$

$n = 4, t = 3$: $0000$

$n = 4, t = 3$: $2022$

(n)
Example radius 1 adaptive packing

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

- 0111 1100
- 1011 0000
- 0010 1011
- 0101 1101
- 0110 1101

(April 29, 2006) Packings within Coverings Combinatorial Challenges ‘06
Example radius 1 adaptive covering

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

Previous packing, plus:

- 0011
- 1110
- 0100
- 0001
- 1001
- 1000

signature = 5, 5, 4, 2
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

- $F'_t(n, 1) := \text{maximum size of packing of 1-sets in } Q_{n,t}$
- $K'_t(n, 1) := \text{minimum size of covering of 1-sets in } Q_{n,t}$
- Sphere bound$^+$.
  
  $F_t(n, 1) \leq F'_t(n, 1) \leq \frac{tn}{1+n(t-1)} \leq K'_t(n, 1) \leq K_t(n, 1)$

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

<table>
<thead>
<tr>
<th>$n$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>$F_2(n, 1)$</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>16</td>
<td>20</td>
<td>40</td>
<td>72</td>
<td>144</td>
</tr>
<tr>
<td>$F'_2(n, 1)$</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>16</td>
<td>28</td>
<td>50</td>
<td>92</td>
<td>170</td>
</tr>
<tr>
<td>$K'_2(n, 1)$</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>10</td>
<td>16</td>
<td>30</td>
<td>52</td>
<td>94</td>
<td>172</td>
</tr>
<tr>
<td>$K_2(n, 1)$</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>7</td>
<td>12</td>
<td>16</td>
<td>32</td>
<td>$\leq 57$</td>
<td>$\leq 105$</td>
<td>$\leq 180$</td>
</tr>
</tbody>
</table>
Liar games defined

2-player perfect information game

- **Players:** Paul – partitioner/questioner
  Carole – chooser/responder

- **n rounds of Game play:**
  - Paul partitions \([m] \rightarrow A_1 \cup \cdots \cup A_t\)
  - Carole selects a part, other parts get 1 lie
  - Elements with \(\leq k\) lies **survive**

Possible winning conditions for Paul

- **Original.** \(\leq 1\) element survives (Rényi, Ulam)
- **Pathological.** \(\geq 1\) 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

Remarks.
Parameters $n$, $t$, $k$ must match!

Many generalizations: attributions $\subseteq 2^{\{Spencer, Yian, Dumitriu, Ellis, Ponomarenko, Nyman\}}$
Equivalence of liar games and packings/coverings

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

- **Online partitions by Paul**
  - Winning strategy in *original game* ↔ *adaptive packing* in hypercube
  - Winning strategy in *pathological game* ↔ *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 $\subseteq 2\{\text{Spencer}, \text{Yan}, \text{Dumitriu}, \text{Ellis}, \text{Ponomarenko}, \text{Nyman}\}$
Sample of previous bounds on adaptive codes

Adaptive packing codes/liar games

- (Berlekamp ‘67) Fixed $k$, weight function
- (Spencer+Winkler ‘91) $k \sim n/3, n/4$ (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⊕{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 \( \{x_2, x_1x_3\} \) 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)
Observation. $t = 2$

arbitrary vertex in $1Q_{3,2}$  1-set in $0Q_{3,2}$
New Contribution

Constructive bottom-up algorithm

Packing within covering **duplication** algorithm

\[
Q_{1,2} \quad \text{duplicate} \quad 0\underbrace{0}_{Q_{1,2}} 1\underbrace{1}_{Q_{1,2}} \quad \text{steal} \quad 0\underbrace{0}_{Q_{1,2}} 1\underbrace{1}_{Q_{1,2}} \quad \rightarrow \quad Q_{2,2}
\]

(April 29, 2006)
Packing within covering **duplication** algorithm

**Q_{1,2}**

- Duplicate: 00 → 00, 01 → 01, 10 → 10, 11 → 11
- Steal: 00 → 00, 01 → 11

**Q_{2,2}**

- Duplicate: 00 → 00, 01 → 01, 11 → 11, 10 → 10
- Steal: 00 → 00, 01 → 11, 10 → 11

**Q_{3,2}**
New Contribution

Constructive bottom-up algorithm

Packing within covering **duplication** algorithm

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

$$
\begin{array}{c|c|c}
Q_{2,2} & 0Q_{2,2} & 1Q_{2,2} \\
3 & 3 & 3 \\
1 & 1 & 1 \\
\end{array}
$$

$$
\begin{array}{c|c|c|c|c|c}
0Q_{2,2} & 1Q_{2,2} & Q_{3,2} & 0Q_{2,2} & 1Q_{2,2} & Q_{3,2} \\
00 & 10 & 00 & 10 & 00 & 10 \\
11 & 11 & 11 & 11 & 11 & 11 \\
01 & 01 & 01 & 01 & 01 & 01 \\
10 & 10 & 10 & 10 & 10 & 10 \\
\end{array}
$$

(April 29, 2006)
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 $F_1, \ldots, F_m$ and a sequence $\alpha_1, \ldots, \alpha_m$ such that for all $J$,

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

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:

{abc, ae, bd, cf}

3, 4, 5, 6 (triangle first)
2, 4, 6, 6 (triangle last)
More counterexamples to having a dominant signature

(V. Asodi) Minimum ground set 3-uniform counterexample

(P. Haxell) Infinite family counterexample with arbitrary prefix difference
New Contribution
Ingredients of the proof

Radius 1 adaptive codes with dominant signatures

Lemma

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

- **Packing:** \( \alpha(n, t, 1) = \cdots = \alpha(n, t, F'_t(n, 1)) = 1 + t(n - 1) \),
- **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

\[
\alpha(n, t, 1) + \alpha(n, t, 2) + \cdots + \alpha(n, t, J) = |F_1 \cup F_2 \cup \cdots \cup F_J|.
\]

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

(April 29, 2006) Packings within Coverings Combinatorial Challenges ‘06 18 / 25
### More iterations of the duplication algorithm

<table>
<thead>
<tr>
<th>$Q_{3,2}$</th>
<th>$0Q_{3,2} 1Q_{3,2}$</th>
<th>$0Q_{3,2} 1Q_{3,2}$</th>
<th>$0Q_{2,2} 1Q_{2,2}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 4</td>
<td>dup. 4 4</td>
<td>st. (a) 5 5</td>
<td>st. (b) 5 5</td>
</tr>
<tr>
<td>4 4</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$Q_{4,2}$</th>
<th>$0Q_{4,2} 1Q_{4,2}$</th>
<th>$0Q_{4,2} 1Q_{4,2}$</th>
<th>$0Q_{4,2} 1Q_{4,2}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 5</td>
<td>dup. 5 5</td>
<td>st. (a) 6 6</td>
<td>st. (b) 6 6</td>
</tr>
<tr>
<td>5 5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4 4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 2</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$Q_{5,2}$</th>
<th>$0Q_{5,2} 1Q_{5,2}$</th>
<th>$0Q_{5,2} 1Q_{5,2}$</th>
<th>$0Q_{5,2} 1Q_{5,2}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 6</td>
<td>dup. 6 6</td>
<td>st. (a) 7 7</td>
<td>st. (b) 7 7</td>
</tr>
<tr>
<td>6 6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6 6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6 6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5 5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 3</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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 $C(n + 1, t, M_0, \ldots, M_{t-1}) :=$

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

(April 29, 2006)
Proving the domination lemma

Proof sketches of the covering and domination lemmas.

• The inner summation is concave; therefore $C(n+1, t, M_0, \ldots, M_{t-1})$ 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 $\beta$ of duplication has $M_0 \geq \cdots \geq M_{t-1} \geq M_0 - 1$.

• Output signature $(\beta(n+1, t, j))_{j \geq 1}$ satisfies for all $K$ (w/abuse),

$$\sum_{j=1}^{K} \beta(n+1, t, j) = C(n+1, t, \lceil K/t \rceil, \ldots, \lfloor K/t \rfloor).$$
Sample case computation for duplication output

Case: • last row which makes a full steal is $r$
  • last nonzero $\beta$ 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 $t \cdot r + 1, \ldots, M$. Then

$$\sum_{j=1}^{M} \beta(n + 1, t, j) = \sum_{j=1}^{tr} (\alpha(n, t, \lceil j/t \rceil) + t - 1) + (M - tr) \left( t^n - \sum_{j=1}^{r} (\alpha(n, t, j) + t - 1) + t - M + tr \right)$$

$$= \sum_{i=1}^{t} \left( \sum_{j=1}^{r} \alpha(n, t, j) + rt - r \right) + (M - tr)(t - (M - tr)) + (M - tr) \left( t^n - \sum_{j=1}^{r} \alpha(n, t, j) - rt + r \right)$$

$$= \sum_{i=1}^{M-tr} t^n + \sum_{i=M-tr+1}^{t} \left( \sum_{j=1}^{r} \alpha(n, t, j) + M - r \right)$$

$$\geq C(n + 1, t, \lceil M/t \rceil, \ldots, \lfloor M/t \rfloor, \lceil M/t \rceil, \ldots, \lfloor M/t \rfloor).$$
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

\[
\begin{array}{c|cc}
 t^{n-1} \mod b_{n,t}(1) & F'_t(n, 1) & K'_t(n, 1) \\
\hline
 i, \ 0 \leq i < t & tS & tS + i \\
 t, \ldots, b_{n-1,t}(1) - 1 & tS & tS + t \\
 b_{n-1,t}(1) - 1 + i, \ 1 \leq i < t & tS + i & tS + t \\
\end{array}
\]

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
- Ahlswede+Cicalese+Deppe. Searching with Lies under Error Cost Constraints
- Ahlswede+Deppe. Non-Binary Error-Correcting Codes with Noiseless Feedback
- Ellis+Nyman. Multichannel Liar Games with a Fixed Number of Lies