INTERNATIONAL MEETING ON NUMERICAL SEMIGROUPS

Numerical Semigroups and Codes

Cortona 2014

José Ignacio Farrán Martín

jifarran@eii.uva.es

Departamento de Matemática Aplicada

Universidad de Valladolid – Campus de Segovia

Escuela Universitaria de Informática

Joint work with: M. Delgado, P. A. García-Sánchez, and D. Llena

Contents

- AG codes
- Numerical semigroups

Contents

- AG codes
- Numerical semigroups

AG codes

Error-correcting codes

- Alphabet $\mathcal{A} = \mathbb{F}_q$
- Code $C \subseteq \mathbb{F}_q^n$
- Dimension $\dim C = k \leq n$
- The difference $n - k$ is called redundancy

Encoding

- Encoding is an injective (linear) map

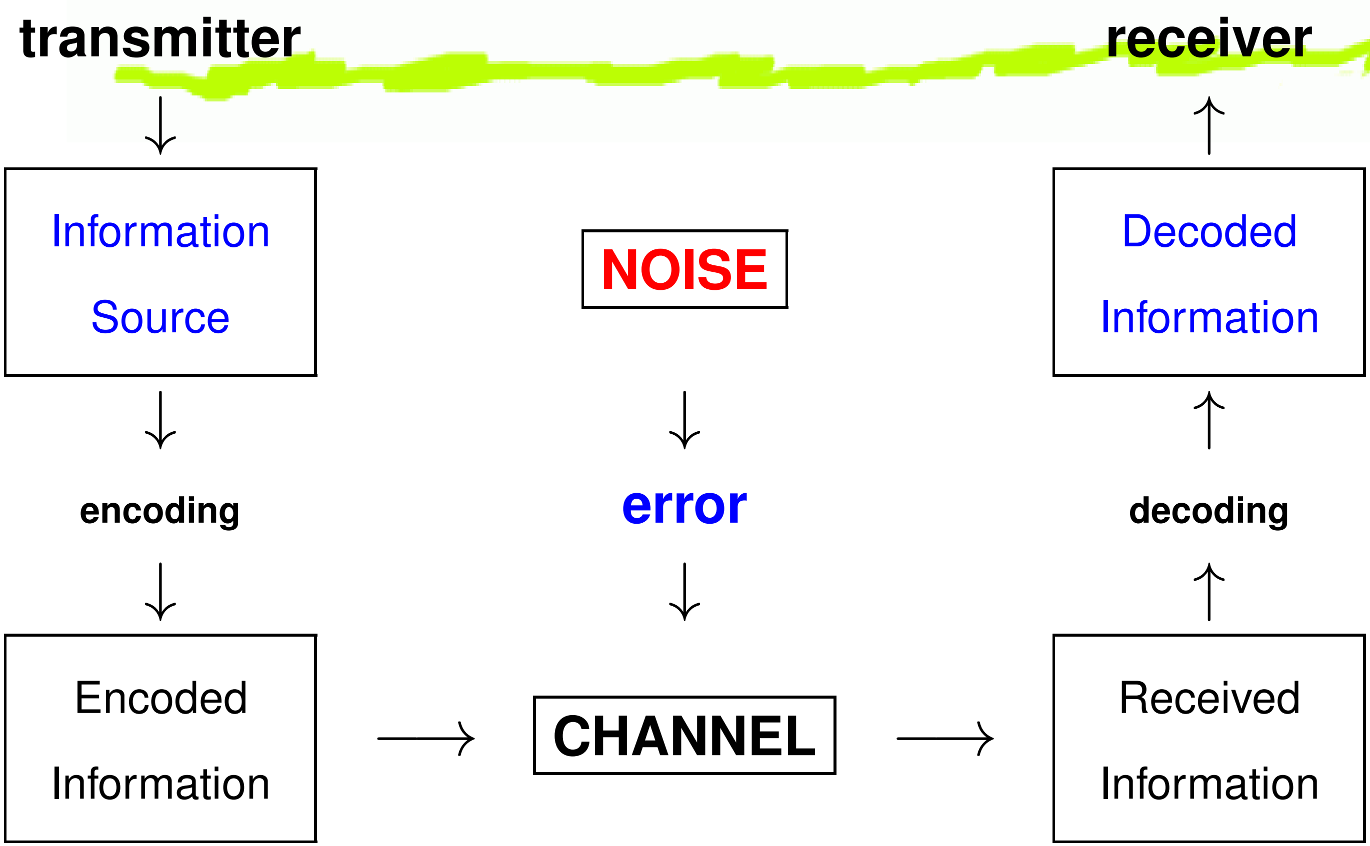
$$\mathcal{C} \ : \ \mathbb{F}_q^k \hookrightarrow \mathbb{F}_q^n$$

  where C is the image of such a map
- It can be described by means of the generator matrix G of C whose rows are a basis of C
- Thus the encoding has a matrix expression

$$\mathbf{c} = \mathbf{m} \cdot G$$

  where $\mathbf{m}$ represents to k “information digits”

Errors


transmitter
receiver
Information Source
NOISE
Decoded Information
encoding
error
decoding
Encoded Information
CHANNEL
Received Information

Examples of codes

source	I	II	III	IV	V
0	0000	00000000	000000000000	00000	00011
1	0001	00000011	000000000111	00011	11000
2	0010	00001100	000000111000	00101	10100
3	0011	00001111	000000111111	00110	01100
4	0100	00110000	000111000000	01001	10010
5	0101	00110011	000111000111	01010	01010
6	0110	00111100	000111111000	01100	00110
7	0111	00111111	000111111111	01111	10001
8	1000	11000000	111000000000	10001	01001
9	1001	11000011	111000000111	10010	00101

Examples of codes

source	I	II	III	IV	V
0	0000	00000000	000000000000	00000	00011
1	0101	00000011	000000000111	00011	11000
2	0010	00001100	000000111000	00101	10100
3	0011	00001111	000000111111	00110	01100
4	0100	00110000	000111000000	01001	10010
5	0101	00110011	000111000111	01010	01010
6	0110	00111100	000111111000	01100	00110
7	0111	00111111	000111111111	01111	10001
8	1000	11000000	111000000000	10001	01001
9	1001	11000011	111000000111	10010	00101

Examples of codes

source	I	II	III	IV	V
0	0000	10000000	000000000000	00000	00011
1	0001	00000011	000000000111	00011	11000
2	0010	00001100	000000111000	00101	10100
3	0011	00001111	000000111111	00110	01100
4	0100	00110000	000111000000	01001	10010
5	0101	00110011	000111000111	01010	01010
6	0110	00111100	000111111000	01100	00110
7	0111	00111111	000111111111	01111	10001
8	1000	11000000	111000000000	10001	01001
9	1001	11000011	111000000111	10010	00101

Examples of codes

source	I	II	III	IV	V
0	0000	00000000	000000000000	00000	00011
1	0001	00000011	000000000010	00011	11000
2	0010	00001100	000000111000	00101	10100
3	0011	00001111	000000111111	00110	01100
4	0100	00110000	000111000000	01001	10010
5	0101	00110011	000111000111	01010	01010
6	0110	00111100	000111111000	01100	00110
7	0111	00111111	000111111111	01111	10001
8	1000	11000000	111000000000	10001	01001
9	1001	11000011	111000000111	10010	00101

Examples of codes

source	I	II	III	IV	V
0	0000	00000000	000000000000	00000	00011
1	0001	00000011	000000000111	00011	11000
2	0010	00001100	000000101000	00101	10100
3	0011	00001111	000000111111	00110	01100
4	0100	00110000	000111000000	01001	10010
5	0101	00110011	000111000111	01010	01010
6	0110	00111100	000111111000	01100	00110
7	0111	00111111	000111111111	01111	10001
8	1000	11000000	111000000000	10001	01001
9	1001	11000011	111000000111	10010	00101

Examples of codes

source	I	II	III	IV	V
0	0000	00000000	000000000000	00000	00011
1	0001	00000011	000000000111	00011	11000
2	0010	00001100	000000111000	00101	10100
3	0011	00001111	000000111111	00110	01100
4	0100	00110000	000111000000	01001	10010
5	0101	00110011	000111000111	01010	01010
6	0110	00111100	000111111000	01100	00110
7	0111	00111111	000111111111	01111	10001
8	1000	11000000	111000000000	10001	01001
9	1001	11000011	111000000111	10010	00101

Examples of codes

source	I	II	III	IV	V
0	0000	00000000	000000000000	01000	00011
1	0001	00000011	000000000111	00011	11000
2	0010	00001100	000000111000	00101	10100
3	0011	00001111	000000111111	00110	01100
4	0100	00110000	000111000000	01001	10010
5	0101	00110011	000111000111	01010	01010
6	0110	00111100	000111111000	01100	00110
7	0111	00111111	000111111111	01111	10001
8	1000	11000000	111000000000	10001	01001
9	1001	11000011	111000000111	10010	00101

Examples of codes

source	I	II	III	IV	V
0	0000	00000000	000000000000	00000	00011
1	0001	00000011	000000000111	00011	11000
2	0010	00001100	000000111000	00101	10100
3	0011	00001111	000000111111	00110	01100
4	0100	00110000	000111000000	01001	10010
5	0101	00110011	000111000111	01010	01010
6	0110	00111100	000111111000	01100	00110
7	0111	00111111	000111111111	01111	10001
8	1000	11000000	111000000000	10001	01001
9	1001	11000011	111000000111	10010	00101

Hamming distance

- The Hamming distance in $\mathbb{F}_q^n$ is defined by

$$d(\mathbf{x},\mathbf{y}) \doteq \sharp\{i \mid x_i \neq y_i\}$$

- The minimum distance of C is

$$d \doteq d(C) \doteq \min\{d(\mathbf{c},\mathbf{c}') \mid \mathbf{c},\mathbf{c}' \in C, \quad \mathbf{c} \neq \mathbf{c}'\}$$

- The parameters of a code are $C \equiv [n,k,d]_q$

length n
dimension k
minimum distance d

Error detection and correction

Let d be the minimum distance of the code C

- C detects up to $d-1$ errors
- C corrects up to $\lfloor\frac{d-1}{2}\rfloor$ errors
- C corrects up to $d-1$ erasures
- C corrects any configuration of t errors and s erasures, provided
$$2t+s\leq d-1$$

Examples

Encode four possible messages $\{a, b, c, d\}$

- Example 1: $n = k = 2$

$$\begin{aligned} a &= 00 \\ b &= 01 \\ c &= 10 \\ d &= 11 \end{aligned}$$

- $d = 1 \Rightarrow$ NO error capability

Examples

Encode four possible messages $\{a, b, c, d\}$

- Example 2: $n = 3$ (one control digit)

$$\begin{aligned} a &= 000 \\ b &= 011 \\ c &= 101 \\ d &= 110 \end{aligned} \qquad (x_3 = x_1 + x_2)$$

- $d = 2 \quad \Rightarrow$ DETECTS one single error

Examples

Encode four possible messages $\{a, b, c, d\}$

- Example 3: $n = 5$ (three control digits)

$$\begin{aligned} a &= 00000 \\ b &= 01101 \\ c &= 10110 \\ d &= 11011 \end{aligned} \qquad \begin{pmatrix} x_3 &= x_1 + x_2 \\ x_4 &= x_2 + x_3 \\ x_5 &= x_3 + x_4 \end{pmatrix}$$

- $d = 3 \quad \Rightarrow \quad$ CORRECTS one single error

Conclusion

It is important for decoding to compute either

- the exact value of d, or
- a lower-bound for d

in order to estimate how many errors (at least) we expect to detect/correct

• In the case of AG codes some numerical semigroup helps . . .

One-point AG Codes

- χ "curve" over a finite field $\mathbb{F} \equiv \mathbb{F}_q$
- P and $P_1, \ldots, P_n$ "rational" points of χ
- C_m^* image of the linear map

$$\begin{array}{rcccl} ev_D & : & \mathcal{L}(mP) & \longrightarrow & \mathbb{F}^n \\ & & f & \mapsto & (f(P_1), \ldots, f(P_n)) \end{array}$$

- C_m the orthogonal code of C_m^*
with respect to the canonical bilinear form

$$\langle \mathbf{a}, \mathbf{b} \rangle \doteq \sum_{i=1}^{n} a_i b_i$$

Parameters

If we assume that $2g - 2 < m < n$, then the encoding

$$\begin{array}{rcl} ev_D \ : \ \mathcal{L}(mP) & \longrightarrow & \mathbb{F}^n \\ f & \mapsto & (f(P_1), \ldots, f(P_n)) \end{array}$$

is injective and

- $k = n - m + g - 1$
- $d \geq m + 2 - 2g$ (Goppa bound)

by using the Riemann-Roch theorem

Weierstrass semigroup

The Goppa bound can actually be improved by using the Weierstrass semigroup of χ at the point p

$$\Gamma_P \doteq \{m \in \mathbb{N} \mid \exists f \;\; \text{with} \;\; (f)_\infty = mP\}$$

Note that $\Gamma_P = \mathbb{N} \setminus \{\ell_1, \ldots, \ell_g\}$ where g is the genus of χ and the numbers ℓ_i are called the Weierstrass gaps of χ at P

- $k = n - k_m$, where $k_m \doteq \sharp(\Gamma_P \cap [0, m])$
  (note that $k_m = m + 1 - g$ for $m >> 0$)
- $d \geq \delta(m+1)$ (the so-called Feng–Rao distance)
- We have an improvement, since
  $\delta(m+1) \geq m + 2 - 2g$, and they coincide for $m >> 0$

Generalized Hamming weights

- Define the support of a linear code C as

$$\mathrm{supp}(C) := \{i \,|\, c_i \neq 0 \text{ for some } \mathbf{c} \in C\}$$

- The r-th generalized weight of C is defined by

$$\mathrm{d}_r(C) := \min\{\sharp\,\mathrm{supp}(C') \mid C' \leq C \text{ with } \dim(C') = r\}$$

- The above definition only makes sense if $r \leq k$, where $k = dim(C)$
- The set of numbers $\mathrm{GHW}(C) := \{\mathrm{d}_1, \ldots, \mathrm{d}_k\}$ is called the weight hierarchy of the code C

Generalized Feng-Rao distances

- It is possible to generalize the generalized Feng-Rao distance for higher order r
- It is also known that for a one-point AG code C_m one has

$$d_r(C_m) \geq \delta_{FR}^r(m+1)$$

- The details on Feng-Rao distances are given later

Griesmer bound

- The generalized weights can also be lower bounded buy a sum depending on the minimum distance:

$$\mathrm{d}_r(C) \geq \sum_{i=0}^{r-1} \left\lceil \frac{\mathrm{d}(C)}{q^i} \right\rceil$$

  where $\mathrm{d}(C) \equiv \mathrm{d}_1(C)$ is the minimum distance of C, which is defined over the finite field $\mathbb{F}_q$

- In particular, for $r = 2$ one has

$$\mathrm{d}_2(C) \geq \mathrm{d}(C) + \left\lceil \frac{\mathrm{d}(C)}{q} \right\rceil$$

Griesmer order bound

- Since we are just using the semigroup for estimating the weight hierarchy of C_m, we can substitute $\mathrm{d}(C_m)$ by the order bound $\delta_{FR}(m+1)$, obtaining

$$\mathrm{d}_r(C_m) \geq \sum_{i=0}^{r-1} \left\lceil \frac{\delta_{FR}(m+1)}{q^i} \right\rceil$$

  We may call this bound the Griesmer order bound

- For $r=2$ this bound becomes

$$\mathrm{d}_2(C) \geq \delta_{FR}(m+1) + \left\lceil \frac{\delta_{FR}(m+1)}{q} \right\rceil$$

  The maximum value is achieved for $q=2$

Contents

- AG codes
- Numerical semigroups

Numerical semigroups

Numerical semigroups

$S \subseteq \mathbb{N}$ such that $\sharp(\mathbb{N} \setminus S) < \infty$ and $0 \in S$

- The genus is $g \doteq \sharp(\mathbb{N} \setminus S)$
- The conductor satisfies $c \leq 2g$
- The last gap is $\ell_g = c - 1$ (Frobenius number)

S is symmetric if $c = 2g$

- First, if we enumerate the elements of S in increasing order
$$S = \{\rho_1 = 0 < \rho_2 < \cdots\}$$
we note that every $m \geq c$ is the $(m + 1 - g)$th element of S, that is $m = \rho_{m+1-g}$

Feng-Rao distance

- The Feng–Rao distance in S is defined as

$$\delta_{FR}(m) := \min\{\nu(m') \mid m' \geq m, \ \ m' \in S\}$$

where $\nu(m') := \sharp N(m')$ and

$$N(m') := \{(a,b) \in S^2 \mid a+b = m'\}$$

Basic results

(i) $\nu(m) = m + 1 - 2g + D(m)$ for $m \geq c$, where

$$D(m) \doteq \sharp\{(x, y) \ \mid \ x, y \notin S \ \text{ and } \ x + y = m\}$$

(ii) $\nu(m) = m + 1 - 2g$ for $m \geq 2c - 1$

(iii) $\delta_{FR}(m) \geq m + 1 - 2g \doteq d^*(m-1) \quad \forall m \in S$,

"and equality holds for $m \geq 2c - 1$"

Two tricks

- Find elements $m \in S$ with $D(m) = 0$

WHY?

(a) $\delta_{FR}(m) = \nu(m) = m + 1 - 2g$ for such elements
(b) For all $m \in S$ one has

$$\delta_{FR}(m) = \min\{\nu(m), \nu(m+1), \ldots, \nu(m')\}$$

where $m' \doteq \min\{r \in S \mid r \geq m \text{ and } D(r) = 0\}$

- Find elements $m \in S$ satisfying the formula

$$\delta_{FR}(m) = \min\{r \in S \mid r \geq m + 1 - 2g\} \qquad [@]$$

Symmetric semigroups

- Theorem: Let S be a symmetric semigroup; then

$$\delta_{FR}(m) = \nu(m) = m - l_g = m + 1 - 2g = e$$

  for all $m = 2g - 1 + e$ with $e \in S \setminus \{0\}$

- Proof: $D(m) = 0$ for such elements

Minimum formula

- For a symmetric semigroup S we can find an element m_0 so that the "minimum formula"

$$\delta_{FR}(m) = \min\{r \in S \mid r \geq m + 1 - 2g\} \qquad [@]$$

in the interval (m_0, ∞) (Campillo and Farrán, with Apéry sets)

  - $S = \langle 9, 12, 15, 17, 20, 23, 25, 28 \rangle$
    $c = 32$ and [@] holds for $m \geq 38$
  - $S = \langle 6, 8, 10, 17, 19 \rangle$
    $c = 22$ and [@] holds for $m \geq 24$

Minimum formula

- For telescopic (free) semigroups, there was an estimate for this m_0 in terms of the generators (Kirfel and Pellikaan)
  - $S = \langle 8, 10, 12, 13 \rangle$

    $c = 28$ and [@] holds for $m \geq 31$
    Instead of $m \geq 42$!
  - $S = \langle 6, 10, 15 \rangle$

    $c = 30$ and [@] holds for $m \geq 30$
    Instead of $m \geq 44$!
- For embedding dimension two numerical semigroups, the minimum formula is true for $m \geq m_0 = c = 2g$

Generalized Feng-Rao distances

- The classical Feng-Rao distance corresponds to $r = 1$ in the following definition:
  - Let S be a numerical semigroup. For any integer $r \geq 1$, the r*-th Feng-Rao distance* of S is defined by

$$\delta^r_{FR}(m) :=$$

$$\min\{\nu(m_1, \ldots, m_r) \mid m \leq m_1 < \cdots < m_r, \ \ m_i \in S\}$$

  - where $\nu(m_1, \ldots, m_r) := \sharp N(m_1, \ldots, m_r)$ and

$$N(m_1, \ldots, m_r) := N(m_1) \cup \cdots \cup N(m_r)$$

Feng-Rao numbers

- There exists a certain constant $E_r = \mathrm{E}(S, r)$, depending on r and S, such that

$$\delta^r_{FR}(m) = m + 1 - 2g + E_r$$

  for $m \geq 2c - 1$

- This constant is called the r*-th Feng-Rao number* of S
- Furthermore, $\delta^r_{FR}(m) \geq m + 1 - 2g + \mathrm{E}(S, r)$ for $m \geq c$, and equality holds if S is symmetric and $m = 2g - 1 + \rho$ for some $\rho \in S \setminus \{0\}$
- We may consider $\mathrm{E}(S, 1) = 0$
- If $g = 0$ then $\mathrm{E}(S, r) = r - 1$

Feng-Rao numbers

We summarize some general properties of the Feng-Rao numbers, for $r \geq 2$ and S fixed, with $g \geq 1$:

1. The function $\mathrm{E}(S, r)$ is non-decreasing in r
2. $r \leq \mathrm{E}(S, r) \leq \rho_r$
3. If furthermore $r \geq c$, then $\mathrm{E}(S, r) = \rho_r = r + g - 1$

Computing the Feng-Rao numbers is very hard, even in very simple examples

- So far, only $\mathrm{E}(S, 2)$ is computed with a general algorithm, based on Apéry sets
- If $S = \langle a, b \rangle$ then $\mathrm{E}(S, 2) = \rho_2$ (by using "deserts")

Embedding dimension two

- In a joint work with M.Delgado, P. García-Sánchez and D. Llena we have recently proved that

$$\mathrm{E}(S, r) = \rho_r$$

- Since embedding dimension two numerical semigroups are symmetric, by using the fact that $\delta^r_{FR}(m) \geq m + 1 - 2g + \mathrm{E}(S, r)$ for $m \geq c$, and that the equality holds if $m = 2g - 1 + \rho_k$ for some $k \geq 2$, one easily obtains the following consequence:

1. $\delta^r_{FR}(m) = \rho_r + \rho_k$ if $m = 2g - 1 + \rho_k$ with $k \geq 2$
2. $\delta^r_{FR}(m) \geq \rho_r + \ell_i$ if $m = 2g - 1 + \ell_i$, where $\ell_i \in \mathrm{G}(S)$ is a gap of S

Improvement

- Our computations improve an old result of Kirfel and Pellikaan, which states

$$\mathrm{d}_r(C_m) \geq \delta_{FR}(m+1) + (r-1).$$

- This inequality is actually a trivial consequence of the inequality $\delta^r_{FR}(m) \geq m + 1 - 2g + \mathrm{E}(S,r)$, by taking into account that $\mathrm{E}(S,r) \geq r-1$
- In fact $\mathrm{E}(S,r) \geq r$ if the genus of S if $g > 0$
- The improvement follows from the fact that $\mathrm{E}(S,r) = \rho_r$ is larger than $r-1$ if $r \geq 2$ and $g \geq 1$

Comparisons

The comparison with the Griesmer order bound depends on q, r and m

- First note a delay, because the bound for C_m corresponds to $m+1$ in S
- On the other hand, note that for $S = \langle a, b \rangle$ the minimum formula $\delta_{FR}(m+1) = \mathrm{min}\{\rho_k \mid \rho_k \geq m+2-2g\}$ holds for $m \geq c$
- Thus, the classical Feng-Rao distance comes in bursts of repeated values, according to intervals of gaps (deserts) of the form $m+2-2g$ preceding the ρ_k that achieves the minimum formula
- As a consequence, the corresponding Griesmer order bound also comes in bursts, and jumps just after the corresponding ρ_k
- Our bound is increasing one by one with m, while the Griesmer order bound jumps at values of m corresponding to gaps of the form $m+2-2g$ starting a desert
- Moreover, when there is no such a gap, the GOB increases by one or more
- Therefore, GOB tends to be better as m becomes large, or if m corresponds to a gap at the beginning of a long desert

Comparisons

Example: $S = \langle 7, 11 \rangle$ and $r = 2$ we obtain with GAP the following results for $q = 2$:

m	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
GFR	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
GOB	11	11	11	11	11	11	17	17	17	17	21	21	21	27	27

Now if $r = 10$:

m	30	31	32	33	34	35	36	37	38	39	40	$\cdots$	50	51	52
GFR	31	32	33	34	35	36	37	38	39	40	41	$\cdots$	51	52	53
GOB	20	20	20	20	20	20	28	28	28	28	33	$\cdots$	49	56	56

Finally, if moreover $q = 16$ then our bound is much better in the whole interval $c \leq m \leq 2c - 1$

Semigroups generated by intervals

If $S = \langle a, a+1, \ldots, a+b \rangle$ the result is not the same, but still we can compute the Feng-Rao numbers

- The trick is again to characterized the so-called amenable sets, which are configurations $m_1 < \cdots < m_r$ with the elements m_i in convenient positions so that the corresponding set of divisors $D(m_1, \ldots, m_r)$ has a minimum cardinality
- To that end, we first note that we can take $m = 2c - 1$, $m_1 = 1$, and combine these two technical results . . .

Semigroups generated by intervals

1. If $0 = i_0 < i_1 < \cdots < i_t < a + b$ then

$$\sharp \mathrm{D}(m, m + i_1, \ldots, m + i_t) \geq \sharp \mathrm{D}(m, m + 1, \ldots, m + t)$$

2. If M is an (S, m, r)-amenable set whose shadow L_M has t elements, then there exists an (S, m, r)-amenable set T whose shadow is an interval containing m, and

$$\sharp \mathrm{D}(T) \leq \sharp \mathrm{D}(M)$$

- For a fixed r, there exists $q \equiv \mathrm{h}(r) \in \mathbb{Z}$ such that

$$q + \frac{1}{2} b q (q - 1) \leq r < 1 + q + \frac{1}{2} b q (q + 1)$$

- By optimizing the position of the vertex of T, one has . . .

Semigroups generated by intervals

- Write r as $r = \mathrm{h}(r) + \frac{1}{2}b\mathrm{h}(r)(\mathrm{h}(r)-1) + k\mathrm{h}(r) + j$ with $-1 \leq k \leq b-1$ and $0 < j \leq \mathrm{h}(r)$
- Then $\mathrm{E}(r, \langle a, a+1, \dots, a+b\rangle)$ equals to

$$r - 1 + \sum_{i=1}^{b(\mathrm{h}(r)-1)+k+1} \left\lceil \frac{a-i}{b} \right\rceil$$

if $b(\mathrm{h}(r)-1)+k+2 < a+b$, and $r - 1 + \sum_{i=1}^{a+b-1} \left\lceil \frac{a-i}{b} \right\rceil$

otherwise

THANK YOU

QUESTIONS?