Davenport and Gao constants for a weighted zero-sum problem with quadratic residues

François Hennecart
(*Institut Camille Jordan Lyon St-Étienne*)

Colloque
Additive Combinatorics in Bordeaux
Université de Bordeaux
11-15 avril 2016

Definitions

Let $R, +, \cdot$ be a finite ring and $A \subset R \setminus \{0\}$.

- **Weighted Davenport constant $D_A(R)$**: least integer such that any sequence S of R with length $\|S\| \geq D_A(R)$ has a (non empty) subsequence $g_1 \cdot g_2 \cdot \cdots \cdot g_\ell$ such that

$$0 \in \sum_{i=1}^{\ell} A g_i \subset \Sigma_A^{(\ell)}(S) := \{A\text{-weighted sums of } \ell \text{ terms of } S\}.$$

Definitions

Let $R, +, \cdot$ be a finite ring and $A \subset R \setminus \{0\}$.

- **Weighted Davenport constant $D_A(R)$**: least integer such that any sequence S of R with length $\|S\| \geq D_A(R)$ has a (non empty) subsequence $g_1 \cdot g_2 \cdot \cdots \cdot g_\ell$ such that

$$0 \in \sum_{i=1}^{\ell} A g_i \subset \Sigma_A^{(\ell)}(S) := \{A\text{-weighted sums of } \ell \text{ terms of } S\}.$$

- **Weighted Gao constant $E_A(R)$**: least integer such that any sequence of R with length $E_A(R)$ has a subsequence $g_1 \cdot g_2 \cdot \cdots \cdot g_{|R|}$ such that

$$0 \in \sum_{i=1}^{|R|} A g_i$$

Definitions

Let $R, +, \cdot$ be a finite ring and $A \subset R \setminus \{0\}$.

- **Weighted Davenport constant $D_A(R)$**: least integer such that any sequence S of R with length $\|S\| \geq D_A(R)$ has a (non empty) subsequence $g_1 \cdot g_2 \cdot \dots \cdot g_\ell$ such that

$$0 \in \sum_{i=1}^{\ell} A g_i \subset \Sigma_A^{(\ell)}(S) := \{A\text{-weighted sums of } \ell \text{ terms of } S\}.$$

- **Weighted Gao constant $E_A(R)$**: least integer such that any sequence of R with length $E_A(R)$ has a subsequence $g_1 \cdot g_2 \cdot \dots \cdot g_{|R|}$ such that

$$0 \in \sum_{i=1}^{|R|} A g_i$$

- **Notation:** for a sequence S of R we denote $\Sigma_A(S)$ all (non empty) A-weighted sums of terms of S. Hence

$$D_A(R) := \min\{k \geq 1 \text{ such that } \|S\| \geq k \Rightarrow 0 \in \Sigma_A(S)\}.$$

Remarks and the fundamental result

- **Remark 1:** $D_A(G)$ and $E_A(G)$ can be defined when $G, +$ is a finite group and $A \subset \mathbf{Z} \setminus \{0\}$.

Remarks and the fundamental result

- **Remark 1:** $D_A(G)$ and $E_A(G)$ can be defined when $G, +$ is a finite group and $A \subset \mathbf{Z} \setminus \{0\}$.
- **Remark 2:** the case $A = \{1\}$ (or any invertible element of R) refers to the classical Davenport and Gao constants, simply denoted by $D(G)$ and $E(G)$.

Remarks and the fundamental result

- **Remark 1:** $D_A(G)$ and $E_A(G)$ can be defined when $G, +$ is a finite group and $A \subset \mathbf{Z} \setminus \{0\}$.
- **Remark 2:** the case $A = \{1\}$ (or any invertible element of R) refers to the classical Davenport and Gao constants, simply denoted by $D(G)$ and $E(G)$.
- **Remark 3:** replacing $|R|$ by $\exp(R)$ for the required length of the subsequence in the definition of $E_A(R)$ leads to the **Erdős-Ginzburg-Ziv constant**.

Remarks and the fundamental result

- **Remark 1:** $D_A(G)$ and $E_A(G)$ can be defined when $G, +$ is a finite group and $A \subset \mathbf{Z} \setminus \{0\}$.
- **Remark 2:** the case $A = \{1\}$ (or any invertible element of R) refers to the classical Davenport and Gao constants, simply denoted by $D(G)$ and $E(G)$.
- **Remark 3:** replacing $|R|$ by $\exp(R)$ for the required length of the subsequence in the definition of $E_A(R)$ leads to the **Erdős-Ginzburg-Ziv constant**.
- **Remark 4:** when $R = \mathbf{Z}/n\mathbf{Z}$ both Gao and Erdős-Ginzburg-Ziv constants coincide.

Remarks and the fundamental result

- **Remark 1:** $D_A(G)$ and $E_A(G)$ can be defined when $G, +$ is a finite group and $A \subset \mathbf{Z} \setminus \{0\}$.
- **Remark 2:** the case $A = \{1\}$ (or any invertible element of R) refers to the classical Davenport and Gao constants, simply denoted by $D(G)$ and $E(G)$.
- **Remark 3:** replacing $|R|$ by $\exp(R)$ for the required length of the subsequence in the definition of $E_A(R)$ leads to the **Erdős-Ginzburg-Ziv constant**.
- **Remark 4:** when $R = \mathbf{Z}/n\mathbf{Z}$ both Gao and Erdős-Ginzburg-Ziv constants coincide.
- **Gao Theorem (1995):** let $G, +$ be an abelian group. Then $\boldsymbol{E(G) = D(G) + |G| - 1}$.

Remarks and the fundamental result

- **Remark 1:** $D_A(G)$ and $E_A(G)$ can be defined when $G, +$ is a finite group and $A \subset \mathbf{Z} \setminus \{0\}$.
- **Remark 2:** the case $A = \{1\}$ (or any invertible element of R) refers to the classical Davenport and Gao constants, simply denoted by $D(G)$ and $E(G)$.
- **Remark 3:** replacing $|R|$ by $\exp(R)$ for the required length of the subsequence in the definition of $E_A(R)$ leads to the **Erdős-Ginzburg-Ziv constant**.
- **Remark 4:** when $R = \mathbf{Z}/n\mathbf{Z}$ both Gao and Erdős-Ginzburg-Ziv constants coincide.
- **Gao Theorem (1995):** let $G, +$ be an abelian group. Then $\boldsymbol{E(G) = D(G) + |G| - 1}$.
- **Grynkiewicz-Marchan-Ordaz Theorem (2012):** $\boldsymbol{E_A(R) = D_A(R) + |R| - 1}$.
  The case $R = \mathbf{Z}/n\mathbf{Z}$ is known since Yuan and Zeng (2010).

Examples

Denote for simplicity $Q^* = Q_n^*$ the set of invertible squares in a given fixed ring R.

- $D(\mathbf{Z}/n\mathbf{Z}) = n$ (**Erdős-Ginzburg-Ziv**).

Examples

Denote for simplicity $Q^* = Q_n^*$ the set of invertible squares in a given fixed ring R.

- $D(\mathbf{Z}/n\mathbf{Z}) = n$ (**Erdős-Ginzburg-Ziv**).
- $D_{Q^*}(\mathbf{Z}/p\mathbf{Z}) = 3$ if $p \geq 7$ is prime.
  Proof. We have $|Q^*| = (p-1)/2$. Then by the Cauchy-Davenport Theorem

  $$|Q^*a + Q^*b + Q^*c| \geq \min(p, 3(p-1)/2 - 2) = p$$

  if a, b, c are not 0. Otherwise we plainly have $0 \in Q^*a \cup Q^*b \cup Q^*c$.

  Conversely take x be a nonsquare modulo p. Then $0 \notin Q^* \cup -Q^*x \cup (Q^* - Q^*x)$. □

Examples

Denote for simplicity $Q^* = Q_n^*$ the set of invertible squares in a given fixed ring R.

- $D(\mathbf{Z}/n\mathbf{Z}) = n$ (**Erdős-Ginzburg-Ziv**).
- $D_{Q^*}(\mathbf{Z}/p\mathbf{Z}) = 3$ if $p \geq 7$ is prime.
  Proof. We have $|Q^*| = (p-1)/2$. Then by the Cauchy-Davenport Theorem

  $$|Q^*a + Q^*b + Q^*c| \geq \min(p, 3(p-1)/2 - 2) = p$$

  if a, b, c are not 0. Otherwise we plainly have $0 \in Q^*a \cup Q^*b \cup Q^*c$.

  Conversely take x be a nonsquare modulo p. Then
  $0 \notin Q^* \cup -Q^*x \cup (Q^* - Q^*x)$. □
- $D_{Q^*}(\mathbf{Z}/3\mathbf{Z}) = D(\mathbf{Z}/3\mathbf{Z}) = 3$.

Examples - continued

- $D_{Q^*}(\mathbf{Z}/5\mathbf{Z}) = D_{\{-1,1\}}(\mathbf{Z}/5\mathbf{Z}) = 3$.
  If a sequence S of $\mathbf{Z}/5\mathbf{Z}$ has length ≥ 3 then
  - either $0 \in S$ and $0 = 1 \cdot 0$;
  - or there exists $x \in S$ such that $-x \in S$: this implies
  $0 = 1 \cdot x + 1 \cdot (-x)$;
  - or S contains two identical terms x, giving $0 = 1 \cdot x + (-1) \cdot x$.

Examples - continued

- $D_{Q^*}(\mathbf{Z}/5\mathbf{Z}) = D_{\{-1,1\}}(\mathbf{Z}/5\mathbf{Z}) = 3.$
  If a sequence S of $\mathbf{Z}/5\mathbf{Z}$ has length ≥ 3 then
  - either $0 \in S$ and $0 = 1 \cdot 0$;
  - or there exists $x \in S$ such that $-x \in S$: this implies $0 = 1 \cdot x + 1 \cdot (-x)$;
  - or S contains two identical terms x, giving $0 = 1 \cdot x + (-1) \cdot x$.
- Write $k = 3q + r$. Then $Q^* = \{1, 9\} + 8\mathbf{Z}/2^k\mathbf{Z}$ and

$$D_{Q^*}(\mathbf{Z}/2^k\mathbf{Z}) = 7q + 2^r = 7\left\lfloor \frac{k}{3} \right\rfloor + 2^{3\{\frac{k}{3}\}}.$$

Examples - continued

- $D_{Q^*}(\mathbf{Z}/5\mathbf{Z}) = D_{\{-1,1\}}(\mathbf{Z}/5\mathbf{Z}) = 3.$
  If a sequence S of $\mathbf{Z}/5\mathbf{Z}$ has length ≥ 3 then
  - either $0 \in S$ and $0 = 1 \cdot 0$;
  - or there exists $x \in S$ such that $-x \in S$: this implies $0 = 1 \cdot x + 1 \cdot (-x)$;
  - or S contains two identical terms x, giving $0 = 1 \cdot x + (-1) \cdot x$.
- Write $k = 3q + r$. Then $Q^* = \{1, 9\} + 8\mathbf{Z}/2^k\mathbf{Z}$ and

$$D_{Q^*}(\mathbf{Z}/2^k\mathbf{Z}) = 7q + 2^r = 7\left\lfloor \frac{k}{3} \right\rfloor + 2^{3\{\frac{k}{3}\}}.$$

- Let $p \geq 3$ be an odd prime number ; then

$$D_{Q^*}(\mathbf{Z}/p^k\mathbf{Z}) = 2k + 1.$$

Examples - continued

- $D_{Q^*}(\mathbf{Z}/5\mathbf{Z}) = D_{\{-1,1\}}(\mathbf{Z}/5\mathbf{Z}) = 3.$
  If a sequence S of $\mathbf{Z}/5\mathbf{Z}$ has length ≥ 3 then
  - either $0 \in S$ and $0 = 1 \cdot 0$;
  - or there exists $x \in S$ such that $-x \in S$: this implies $0 = 1 \cdot x + 1 \cdot (-x)$;
  - or S contains two identical terms x, giving $0 = 1 \cdot x + (-1) \cdot x$.
- Write $k = 3q + r$. Then $Q^* = \{1, 9\} + 8\mathbf{Z}/2^k\mathbf{Z}$ and

$$D_{Q^*}(\mathbf{Z}/2^k\mathbf{Z}) = 7q + 2^r = 7\left\lfloor \frac{k}{3} \right\rfloor + 2^{3\{\frac{k}{3}\}}.$$

- Let $p \geq 3$ be an odd prime number ; then

$$D_{Q^*}(\mathbf{Z}/p^k\mathbf{Z}) = 2k + 1.$$

- **Question:** is it true that if $\gcd(n, 2) = 1$ then $D_{Q^*}(\mathbf{Z}/n\mathbf{Z}) = 2\Omega(n) + 1$?

A critical situation

Assume that $n = 15$ and let $S = (1, 1, 1, 1, 1)$. One has $Q^* = \{1, 4\}$ and consequently

$$\mathbf{0} \notin \boldsymbol{\Sigma}_{\boldsymbol{Q^*}}(\boldsymbol{S}) \;!$$

We have $D_{Q^*}(\mathbf{Z}/15\mathbf{Z}) > 5 = 2\Omega(15) + 1$.

A critical situation

Assume that $n = 15$ and let $S = (1, 1, 1, 1, 1)$. One has $Q^* = \{1, 4\}$ and consequently

$$\mathbf{0} \notin \boldsymbol{\Sigma}_{\boldsymbol{Q^*}}(\boldsymbol{S}) \ !$$

We have $D_{Q^*}(\mathbf{Z}/15\mathbf{Z}) > 5 = 2\Omega(15) + 1$.

- **Remark:** the primes $2, 3$ and 5 play a *bad* role.

A critical situation

Assume that $n = 15$ and let $S = (1,1,1,1,1)$. One has $Q^* = \{1,4\}$ and consequently

$$\mathbf{0} \notin \boldsymbol{\Sigma}_{Q^*}(\boldsymbol{S}) \ !$$

We have $D_{Q^*}(\mathbf{Z}/15\mathbf{Z}) > 5 = 2\Omega(15) + 1$.

- **Remark:** the primes $2, 3$ and 5 play a *bad* role.
- **An attempt of conjecture:** if $\gcd(n,2) = 1$ and n is not a multiple of 15 then $D_{Q^*}(\mathbf{Z}/n\mathbf{Z}) = 2\Omega(n) + 1$.

A critical situation

Assume that $n = 15$ and let $S = (1, 1, 1, 1, 1)$. One has $Q^* = \{1, 4\}$ and consequently

$$\mathbf{0} \notin \boldsymbol{\Sigma}_{\boldsymbol{Q^*}}(\boldsymbol{S}) \; !$$

We have $D_{Q^*}(\mathbf{Z}/15\mathbf{Z}) > 5 = 2\Omega(15) + 1$.

- **Remark:** the primes $2, 3$ and 5 play a *bad* role.
- **An attempt of conjecture:** if $\gcd(n, 2) = 1$ and n is not a multiple of 15 then $D_{Q^*}(\mathbf{Z}/n\mathbf{Z}) = 2\Omega(n) + 1$.
- **Theorem (Chintamani-Moriya, 2012)**: if $\gcd(n, 30) = 1$ then $D_{Q^*}(\mathbf{Z}/n\mathbf{Z}) = 2\Omega(n) + 1$.

A critical situation

Assume that $n = 15$ and let $S = (1, 1, 1, 1, 1)$. One has $Q^* = \{1, 4\}$ and consequently

$$\mathbf{0} \notin \boldsymbol{\Sigma}_{Q^*}(\boldsymbol{S}) \text{ !}$$

We have $D_{Q^*}(\mathbf{Z}/15\mathbf{Z}) > 5 = 2\Omega(15) + 1$.

- **Remark:** the primes $2, 3$ and 5 play a *bad* role.
- **An attempt of conjecture:** if $\gcd(n, 2) = 1$ and n is not a multiple of 15 then $D_{Q^*}(\mathbf{Z}/n\mathbf{Z}) = 2\Omega(n) + 1$.
- **Theorem (Chintamani-Moriya, 2012)**: if $\gcd(n, 30) = 1$ then $D_{Q^*}(\mathbf{Z}/n\mathbf{Z}) = 2\Omega(n) + 1$.
- The proof uses an **inductive argument** and **an addition theorem**:

A critical situation

Assume that $n = 15$ and let $S = (1, 1, 1, 1, 1)$. One has $Q^* = \{1, 4\}$ and consequently

$$\mathbf{0} \notin \boldsymbol{\Sigma}_{Q^*}(\boldsymbol{S}) \text{ !}$$

We have $D_{Q^*}(\mathbf{Z}/15\mathbf{Z}) > 5 = 2\Omega(15) + 1$.

- **Remark:** the primes $2, 3$ and 5 play a *bad* role.
- **An attempt of conjecture:** if $\gcd(n, 2) = 1$ and n is not a multiple of 15 then $D_{Q^*}(\mathbf{Z}/n\mathbf{Z}) = 2\Omega(n) + 1$.
- **Theorem (Chintamani-Moriya, 2012)**: if $\gcd(n, 30) = 1$ then $D_{Q^*}(\mathbf{Z}/n\mathbf{Z}) = 2\Omega(n) + 1$.
- The proof uses an **inductive argument** and **an addition theorem**:
- **Chowla Theorem:** if $X \subset \mathbf{Z}/n\mathbf{Z}$ and $Y \subset \left(\mathbf{Z}/n\mathbf{Z}\right)^\times$ then

$$|X + Y| \geq \min(n, |X| + |Y| - 1).$$

Idea of the proof (upper bound)

Let S be a sequence of length $\|S\| = 2\Omega(n) + 1$.

- **First case:** if for some $p \mid n$, S has at most two terms non divisible by p then one applies the induction hypothesis to $S' := \frac{1}{p} \times \tilde{S}$ where $\tilde{S}$ is the subsequence of S formed by the terms divisible by p: S' can be viewed has a sequence of $\mathbf{Z}/m\mathbf{Z}$ where $m = n/p$ with length $\geq 2\Omega(n) + 1 - 2 = 2\Omega(m) + 1$.

Idea of the proof (upper bound)

Let S be a sequence of length $\|S\| = 2\Omega(n) + 1$.

- **First case:** if for some $p \mid n$, S has at most two terms non divisible by p then one applies the induction hypothesis to $S' := \frac{1}{p} \times \tilde{S}$ where $\tilde{S}$ is the subsequence of S formed by the terms divisible by p: S' can be viewed has a sequence of $\mathbf{Z}/m\mathbf{Z}$ where $m = n/p$ with length $\geq 2\Omega(n) + 1 - 2 = 2\Omega(m) + 1$.
- **Second case:** for each $p \mid n$, S has at least 3 terms coprime to p. There are $p^k(p-1)/2$ square units modulo p^k. Hence if $p \nmid abc$, by Chowla Theorem $\left| Q^*_{p^k} a + Q^*_{p^k} b + Q^*_{p^k} c \right| = p^k$, that is

$$Q^*_{p^k} a + Q^*_{p^k} b + Q^*_{p^k} c = \mathbf{Z}/p^k\mathbf{Z}.$$

By the Chinese remainder Theorem, taking the minimal subsequence $s_1 \cdot \dots \cdot s_\ell$ of S containing 3 terms coprime to p for each $p \mid n$, one has

$$\sum_{i=1}^{\ell} Q^*_n s_i = \mathbf{Z}/n\mathbf{Z} \quad \text{hence} \quad 0 \in \sum_{i=1}^{\ell} Q^*_n s_i.$$

Main results

- **Theorem 1 (Grynkiewicz-H., 2015)**
  If $\gcd(n, 6) = 1$ or $\gcd(n, 10) = 1$ then $D_{Q^*}(\mathbf{Z}/n\mathbf{Z}) = 2\Omega(n) + 1$.

Main results

- **Theorem 1 (Grynkiewicz-H., 2015)**
  If $\gcd(n, 6) = 1$ or $\gcd(n, 10) = 1$ then $D_{Q^*}(\mathbf{Z}/n\mathbf{Z}) = 2\Omega(n) + 1$.
- **Theorem 2 (Grynkiewicz-H., 2015)**
  If n is an odd integer then

$$2\Omega(n) + 1 + \min(v_3(n), v_5(n)) \leq D_{Q^*}(\mathbf{Z}/n\mathbf{Z}) \leq 2\Omega(n) + 1 + v_5(n).$$

Main results

- **Theorem 1 (Grynkiewicz-H., 2015)**
  If $\gcd(n, 6) = 1$ or $\gcd(n, 10) = 1$ then $D_{Q^*}(\mathbf{Z}/n\mathbf{Z}) = 2\Omega(n) + 1$.
- **Theorem 2 (Grynkiewicz-H., 2015)**
  If n is an odd integer then

$$2\Omega(n) + 1 + \min(v_3(n), v_5(n)) \leq D_{Q^*}(\mathbf{Z}/n\mathbf{Z}) \leq 2\Omega(n) + 1 + v_5(n).$$

- **Corollary**: for any odd integer n, the exact value of $D_{Q^*}(\mathbf{Z}/n\mathbf{Z})$ is known when $n = qm$ where $\gcd(m, 30) = 1$ and $q = 3^k$ or 5^k or 15^k.

Main results

- **Theorem 1 (Grynkiewicz-H., 2015)**
  If $\gcd(n,6)=1$ or $\gcd(n,10)=1$ then $D_{Q^*}(\mathbf{Z}/n\mathbf{Z}) = 2\Omega(n)+1$.
- **Theorem 2 (Grynkiewicz-H., 2015)**
  If n is an odd integer then

$$2\Omega(n)+1+\min(v_3(n),v_5(n)) \leq D_{Q^*}(\mathbf{Z}/n\mathbf{Z}) \leq 2\Omega(n)+1+v_5(n).$$

- **Corollary**: for any odd integer n, the exact value of $D_{Q^*}(\mathbf{Z}/n\mathbf{Z})$ is known when $n=qm$ where $\gcd(m,30)=1$ and $q=3^k$ or 5^k or 15^k.
- **Reformulation of Theorem 1 when $\gcd(n,6)=1$:**
  if $m \geq 3\omega(n)+\min(1,v_5(n))$ then for all sequence S of $\mathbf{Z}/n\mathbf{Z}$ with length $m+2\Omega(n)$

$$0 \in \Sigma_{Q^*}^{(m)}(S).$$

  Taking $m=n$ gives the Gao constant $E_{Q^*}(\mathbf{Z}/n\mathbf{Z}) = n+2\Omega(n)$ when $n \geq 3\omega(n)+\min(1,v_5(n))$ (namely when $n \geq 5$) and $\gcd(n,6)=1$.

Lower bound

- If $p \geq 3$ is a prime number then

$$D_{Q^*}(\mathbf{Z}/p^k\mathbf{Z}) = 2k + 1.$$

Lower bound

- If $p \geq 3$ is a prime number then

$$D_{Q^*}(\mathbf{Z}/p^k\mathbf{Z}) = 2k + 1.$$

- For any pair of positive integers m, n

$$D_{Q^*}(\mathbf{Z}/mn\mathbf{Z}) \geq D_{Q^*}(\mathbf{Z}/m\mathbf{Z}) + D_{Q^*}(\mathbf{Z}/n\mathbf{Z}) - 1.$$

Lower bound

- If $p \geq 3$ is a prime number then

$$D_{Q^*}(\mathbf{Z}/p^k\mathbf{Z}) = 2k + 1.$$

- For any pair of positive integers m, n

$$D_{Q^*}(\mathbf{Z}/mn\mathbf{Z}) \geq D_{Q^*}(\mathbf{Z}/m\mathbf{Z}) + D_{Q^*}(\mathbf{Z}/n\mathbf{Z}) - 1.$$

- When $\gcd(n, 6) = 1$ or $\gcd(n, 10) = 1$ write

$$n = \prod_{i=1}^{s} p_i^{k_i}, \quad k_i := v_{p_i}(n).$$

- When $15 \mid n$ write

$$n = 15^k \prod_{i=1}^{s} p_i^{k_i}$$

and observe that $D_{Q^*}(\mathbf{Z}/15^k\mathbf{Z}) \geq 5k + 1.$

Upper bound

- When $5 \mid n$, we use sharper addition theorems instead of Chowla's theorem.

Upper bound

- When $5 \mid n$, we use sharper addition theorems instead of Chowla's theorem.
- The case $\gcd(n, 6) = 1$ can be managed by induction in a similar way as for $\gcd(n, 30) = 1$.

Upper bound

- When $5 \mid n$, we use sharper addition theorems instead of Chowla's theorem.
- The case $\gcd(n, 6) = 1$ can be managed by induction in a similar way as for $\gcd(n, 30) = 1$.
- The general case needs an additional combinatorial tool based on the study of the hypergraph structure of the sequences.

Admissible functions and stable sequences

Let $G = \mathbf{Z}/n\mathbf{Z}$.

A function $f : \{\text{subgroups of } G\} \to \mathbf{Z}_+^*$ is said to be **admissible** if

- f is **strongly increasing**: $H < H' \leq G \Longrightarrow f(H) \leq f(H') - 2$,
- f is **subadditive**: $f(H + H') \leq f(H) + f(H') - f(H \cap H')$ for $H, H' \leq G$.

Admissible functions and stable sequences

Let $G = \mathbf{Z}/n\mathbf{Z}$.

A function $f : \{\text{subgroups of } G\} \to \mathbf{Z}_+^*$ is said to be **admissible** if

- f is **strongly increasing**: $H < H' \leq G \implies f(H) \leq f(H') - 2$,
- f is **subadditive**: $f(H + H') \leq f(H) + f(H') - f(H \cap H')$ for $H, H' \leq G$.

  - Example 1: $f(H) = m + 2\Omega(|H|)$ is admissible.

Admissible functions and stable sequences

Let $G = \mathbf{Z}/n\mathbf{Z}$.

A function $f : \{\text{subgroups of } G\} \to \mathbf{Z}_+^*$ is said to be **admissible** if

- f is **strongly increasing**: $H < H' \leq G \implies f(H) \leq f(H') - 2$,
- f is **subadditive**: $f(H + H') \leq f(H) + f(H') - f(H \cap H')$ for $H, H' \leq G$.

- Example 1: $f(H) = m + 2\Omega(|H|)$ is admissible.
- Example 2: if f is admissible and $K < G$, then $f_K(H) = f(H + K)$ is admissible.

Admissible functions and stable sequences

Let $G = \mathbf{Z}/n\mathbf{Z}$.

A function $f : \{\text{subgroups of } G\} \to \mathbf{Z}_+^*$ is said to be **admissible** if

- f is **strongly increasing**: $H < H' \leq G \Longrightarrow f(H) \leq f(H') - 2$,
- f is **subadditive**: $f(H + H') \leq f(H) + f(H') - f(H \cap H')$ for $H, H' \leq G$.
  - Example 1: $f(H) = m + 2\Omega(|H|)$ is admissible.
  - Example 2: if f is admissible and $K < G$, then $f_K(H) = f(H + K)$ is admissible.

A sequence S of G of length $\|S\| \geq f(G)$ is said to be ***f*-stable** with respect to G if

- S generates G,
- $\|S\| - \|S_H\| \geq f(G) - f(H) + 1$ for all subgroups $H < G$,

where S_E denotes the subsequence of S of all terms of S belonging to E.

Admissible functions and stable sequences

Let $G = \mathbf{Z}/n\mathbf{Z}$.

A function $f : \{\text{subgroups of } G\} \to \mathbf{Z}_+^*$ is said to be **admissible** if

- f is **strongly increasing**: $H < H' \le G \implies f(H) \le f(H') - 2$,
- f is **subadditive**: $f(H + H') \le f(H) + f(H') - f(H \cap H')$ for $H, H' \le G$.

  - Example 1: $f(H) = m + 2\Omega(|H|)$ is admissible.
  - Example 2: if f is admissible and $K < G$, then $f_K(H) = f(H + K)$ is admissible.

A sequence S of G of length $\|S\| \ge f(G)$ is said to be $\boldsymbol{f}$**-stable** with respect to G if

- S generates G,
- $\|S\| - \|S_H\| \ge f(G) - f(H) + 1$ for all subgroups $H < G$,

where S_E denotes the subsequence of S of all terms of S belonging to E.

Remark: when S is not f-stable, the induction works pretty well.

Structure for f-stable sequences

- An ***f*-component** of S is a subsequence V of S satisfying
  - $S \setminus V$ is f-stable with respect to $H := \langle S \setminus V \rangle$,
  - $\|V\| \leq f(G) - f(H) + 1$.

Structure for f-stable sequences

- An ***f*-component** of S is a subsequence V of S satisfying
  - $S \setminus V$ is f-stable with respect to $H := \langle S \setminus V \rangle$,
  - $\|V\| \leq f(G) - f(H) + 1$.
- **Proposition:** any f-stable sequence S can be decomposed as a disjoint union

$$S = V_1 \cdot V_2 \cdot \cdots \cdot V_r$$

  of f-components V_i.

Structure for f-stable sequences

- An ***f*-component** of S is a subsequence V of S satisfying
  - $S \setminus V$ is f-stable with respect to $H := \langle S \setminus V \rangle$,
  - $\|V\| \leq f(G) - f(H) + 1$.
- **Proposition:** any f-stable sequence S can be decomposed as a disjoint union
$$S = V_1 \cdot V_2 \cdot \cdots \cdot V_r$$
  of f-components V_i.
- An ***f*-near component** of S is a subsequence E of S satisfying
  - $S \setminus E$ is f-stable with respect to $H := \langle S \setminus E \rangle$,
  - $\|E\| \leq f(G) - f(H) + 2$,
  - E is maximal for inclusion (as a subsequence of S).

Structure for f-stable sequences

- An ***f*-component** of S is a subsequence V of S satisfying
  - $S \setminus V$ is f-stable with respect to $H := \langle S \setminus V \rangle$,
  - $\|V\| \leq f(G) - f(H) + 1$.
- **Proposition:** any f-stable sequence S can be decomposed as a disjoint union

$$S = V_1 \cdot V_2 \cdot \cdots \cdot V_r$$

  of f-components V_i.
- An ***f*-near component** of S is a subsequence E of S satisfying
  - $S \setminus E$ is f-stable with respect to $H := \langle S \setminus E \rangle$,
  - $\|E\| \leq f(G) - f(H) + 2$,
  - E is maximal for inclusion (as a subsequence of S).
- **Proposition:** any f-near component f S is a disjoint union of f-components of S:

$$E = V_{i_1} \cdot V_{i_2} \cdot \cdots \cdot V_{i_t}.$$

Pairwise balanced design

We assume $3 \mid n$.

- **Definition:** an hypergraph is a **pairwise balanced design** if each pair of vertices belongs to exactly λ edges.

Pairwise balanced design

We assume $3 \mid n$.

- **Definition:** an hypergraph is a **pairwise balanced design** if each pair of vertices belongs to exactly λ edges.
- **Theorem (DG-FH, 2015):**
  The hypergraph $\mathcal{H} = (\{f\text{-components}\}, \{f\text{-near components}\})$ is a pairwise balanced design with $\lambda = 1$.

Pairwise balanced design

We assume $3 \mid n$.

- **Definition:** an hypergraph is a **pairwise balanced design** if each pair of vertices belongs to exactly λ edges.
- **Theorem (DG-FH, 2015):**
  The hypergraph $\mathcal{H} = (\{f\text{-components}\}, \{f\text{-near components}\})$ is a pairwise balanced design with $\lambda = 1$.
- **Classical lemma:** let

$$\mathcal{E} = \{\text{number of edges in } E,\ E \text{ is a } f\text{-near component of } S\}$$

and $e = \gcd\{k(k-1),\ k \in \mathcal{E}\}$. Then

$$v(v-1) \equiv 0 \pmod{e}.$$

Application

Let $S = W \cdot 0^{\|S\|-m}$ with $W = V_1 \cdot V_2 \cdot \cdots \cdot V_r$ with $\|W\| = m$, where the V_i's are f-components. Write $\sigma(T)$ for the sum of all terms of a given sequence T.

Application

Let $S = W \cdot 0^{\|S\|-m}$ with $W = V_1 \cdot V_2 \cdot \dots \cdot V_r$ with $\|W\| = m$, where the V_i's are f-components. Write $\sigma(T)$ for the sum of all terms of a given sequence T.
Assume $\sigma(S) = \sigma(W) \equiv x \pmod{G/3G}$ with $x \neq 0$ (otherwise we can conclude).

Application

Let $S = W \cdot 0^{\|S\|-m}$ with $W = V_1 \cdot V_2 \cdot \cdots \cdot V_r$ with $\|W\| = m$, where the V_i's are f-components. Write $\sigma(T)$ for the sum of all terms of a given sequence T.

Assume $\sigma(S) = \sigma(W) \equiv x \pmod{G/3G}$ with $x \neq 0$ (otherwise we can conclude).

If for some i, $\sigma(V_i) \equiv x \pmod{G/3G}$ then $\sigma(W \setminus V_i) \equiv 0 \pmod{G/3G}$ and we can conclude.

Application

Let $S = W \cdot 0^{\|S\|-m}$ with $W = V_1 \cdot V_2 \cdot \dots \cdot V_r$ with $\|W\| = m$, where the V_i's are f-components. Write $\sigma(T)$ for the sum of all terms of a given sequence T.
Assume $\sigma(S) = \sigma(W) \equiv x \pmod{G/3G}$ with $x \neq 0$ (otherwise we can conclude).
If for some i, $\sigma(V_i) \equiv x \pmod{G/3G}$ then $\sigma(W \setminus V_i) \equiv 0 \pmod{G/3G}$ and we can conclude.
Let v the number of V_i's such that $\sigma(V_i) \equiv -x \pmod{G/3G}$. Then

$$x \equiv -vx \pmod{3} \quad \text{thus} \quad v \equiv -1 \pmod{3}.$$

Application

Let $S = W \cdot 0^{\|S\|-m}$ with $W = V_1 \cdot V_2 \cdot \dots \cdot V_r$ with $\|W\| = m$, where the V_i's are f-components. Write $\sigma(T)$ for the sum of all terms of a given sequence T.

Assume $\sigma(S) = \sigma(W) \equiv x \pmod{G/3G}$ with $x \neq 0$ (otherwise we can conclude).

If for some i, $\sigma(V_i) \equiv x \pmod{G/3G}$ then $\sigma(W \setminus V_i) \equiv 0 \pmod{G/3G}$ and we can conclude.

Let v the number of V_i's such that $\sigma(V_i) \equiv -x \pmod{G/3G}$. Then

$$x \equiv -vx \pmod{3} \quad \text{thus} \quad v \equiv -1 \pmod{3}.$$

Each edge of $\mathcal{H}$ has 0 or 1 $\pmod{3}$ vertices. Hence $e \equiv 0 \pmod{6}$.

Application

Let $S = W \cdot 0^{\|S\|-m}$ with $W = V_1 \cdot V_2 \cdot \cdots \cdot V_r$ with $\|W\| = m$, where the V_i's are f-components. Write $\sigma(T)$ for the sum of all terms of a given sequence T.
Assume $\sigma(S) = \sigma(W) \equiv x \pmod{G/3G}$ with $x \neq 0$ (otherwise we can conclude).
If for some i, $\sigma(V_i) \equiv x \pmod{G/3G}$ then $\sigma(W \setminus V_i) \equiv 0 \pmod{G/3G}$ and we can conclude.
Let v the number of V_i's such that $\sigma(V_i) \equiv -x \pmod{G/3G}$. Then

$$x \equiv -vx \pmod 3 \quad \text{thus} \quad v \equiv -1 \pmod 3.$$

Each edge of $\mathcal{H}$ has 0 or 1 $\pmod 3$ vertices. Hence $e \equiv 0 \pmod 6$.
A contradiction !

Final remarks

Final remarks

- **Conjecture 1:** for all odd integer $n \geq 3$

$$D_{Q^*}(\mathbf{Z}/n\mathbf{Z}) = 2\Omega(n) + \min(v_3(n), v_5(n)) + 1.$$

Final remarks

- **Conjecture 1:** for all odd integer $n \geq 3$

$$D_{Q^*}(\mathbf{Z}/n\mathbf{Z}) = 2\Omega(n) + \min(v_3(n), v_5(n)) + 1.$$

- **Conjecture 2:** for all odd integer $n \geq 3$, all integer $m \geq \text{cste} \times \Omega(n)$ divisible by $\gcd(n, 3)$ and all sequence S of $\mathbf{Z}/n\mathbf{Z}$

$$\|S\| \geq m + 2\Omega(n) + \min(v_3(n), v_5(n)) \Longrightarrow 0 \in \Sigma_{Q^*}^{(m)}(S).$$

Final remarks

- **Conjecture 1:** for all odd integer $n \geq 3$

$$D_{Q^*}(\mathbf{Z}/n\mathbf{Z}) = 2\Omega(n) + \min(v_3(n), v_5(n)) + 1.$$

- **Conjecture 2:** for all odd integer $n \geq 3$, all integer $m \geq \text{cste} \times \Omega(n)$ divisible by $\gcd(n, 3)$ and all sequence S of $\mathbf{Z}/n\mathbf{Z}$

$$\|S\| \geq m + 2\Omega(n) + \min(v_3(n), v_5(n)) \Longrightarrow 0 \in \Sigma_{Q^*}^{(m)}(S).$$

- **Conjecture 3:** for all odd integer $n \geq 3$

$$D_{Q^*}(\mathbf{Z}/2^k n\mathbf{Z}) = 7\left\lfloor \frac{k}{3} \right\rfloor + 2^{3\{\frac{k}{3}\}} + 2\Omega(n) + \min(v_3(n), v_5(n)).$$

Thank you for your attention