ALCOMA2015, Kloster Banz, Germany, 2015.

q-Analogue of Cyclic Binary Sequences

Netanel Raviv

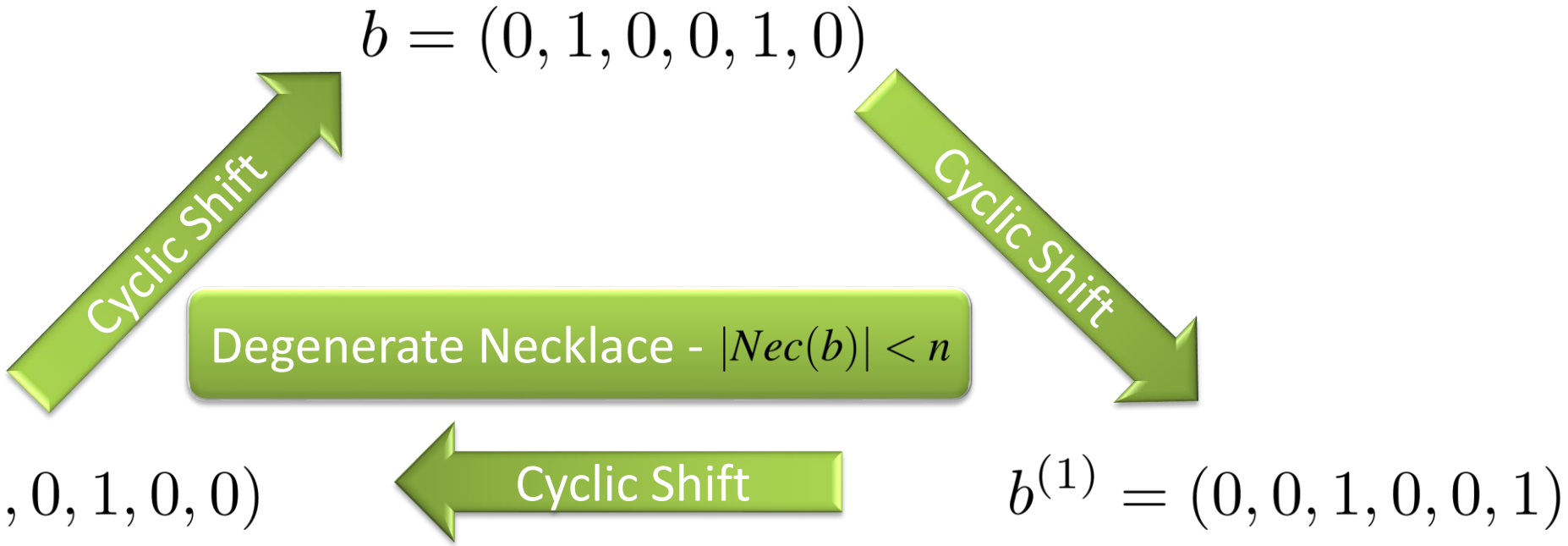
Joint work with:

Prof. Tuvi Etzion

Technion, Israel

Cyclic Binary Sequences – Preliminaries

- Let $b \in \{0,1\}^n, b = (b_0, \ldots, b_{n-1})$.
- A cyclic shift of b is $b^{(i)} = (b_{n-i}, \ldots, b_{n-1}, b_0, \ldots, b_{n-i-1})$.
- The necklace of b is $Nec(b) \triangleq \{b^{(i)} | i \in \mathbb{N}\}$.



q-Analogue of Cyclic Binary Sequences - Overview

Goal – Adapt existing results about CBS to their q-analogues.

Cyclic Binary Sequences

- Cyclic shift of a binary sequences.
- Necklace.
- Possible sizes of a necklace.
  - (Non-)Degenerate necklaces.
- Enumeration of full necklaces using the Möbius Inversion Theorem.

Cyclic Subspaces

- Cyclic shift of a subspace.
- Orbit.
- Possible sizes of an orbit.
  - Structure of all degenerate orbits.
- Enumeration of full orbits using the Möbius Inversion Theorem.

- Solution by [Drudge02]

Cyclic Subspaces – Preliminaries

$Orb(V) \triangleq \{\alpha V | \alpha \in \mathbb{F}_{q^n}^*\}$

- $\mathcal{G}_q(n,k)$ - The set of all k-subspaces of $\mathbb{F}_{q^n}$.
- Fix $\gamma \in \mathbb{F}_{q^n}$, a primitive element, and let $V \in \mathcal{G}_q(n,k)$.
- γ, V admit a characteristic vector w.r.t $\mathbb{F}_{q^n}$.

$$b_V \triangleq \left(\overset{\gamma^0}{0}, \overset{\gamma}{1}, \overset{\gamma^2}{0}, \overset{\gamma^3}{0}, \cdots, \overset{\gamma^{q^n-2}}{1} \right)$$

- For any $\alpha \in \mathbb{F}_{q^n}^*$, let $\alpha V \triangleq \{\alpha \cdot v | v \in V\}$. Clearly, $\alpha V \in \mathcal{G}_q(n,k)$.
- If $\alpha = \gamma^j$, then $b_{\alpha V} = b_V^{(j)}$.
- E.g., $\alpha = \gamma^2$, $b_{\alpha V} \triangleq \left(\overset{\gamma^0}{0}, \overset{\gamma}{1}, \overset{\gamma^2}{0}, \overset{\gamma^3}{1}, \cdots, \overset{\gamma^{q^n-2}}{0} \right)$

Cyclic Subspaces – Motivation

- Several *small* examples for good subspace codes turned out to be *cyclic*:

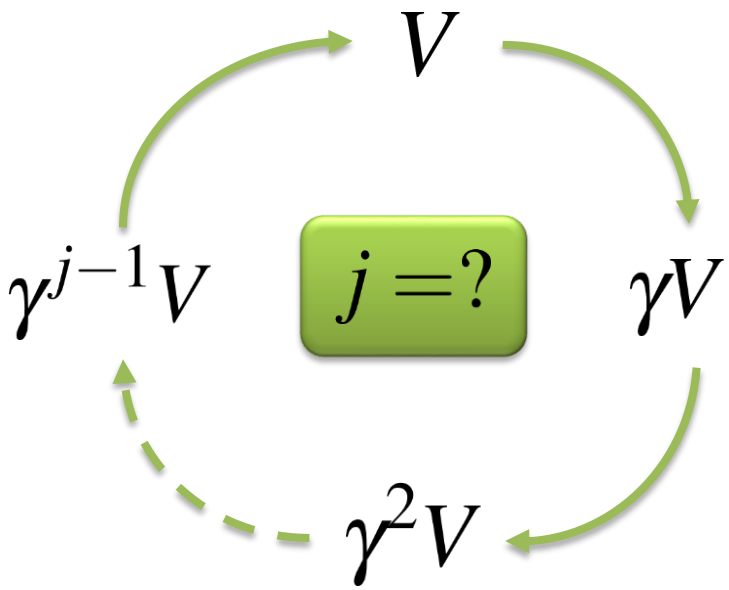
A. Kohnert and S. Kurz: Construction of large constant dimension codes with a prescribed minimum distance, Lecture Notes Computer Science, 5393, 31-42, (2008)

M. Braun, T. Etzion, P. R. J. Ostergard, A. Vardy, and A. Wassermann: Existence of q-Analogs of Steiner Systems, arxiv.org/abs/1304.1462, (2013)

T. Etzion, A. Vardy: Error-correcting codes in projective space. IEEE Transactions on Information Theory, vol. 57(2), 1165-1173, (2011)

Possible Necklace/Orbit Sizes.

- Let $|Nec(b)| = j$. Then, $b^{(n)} = b = b^{(j)}$.
- Therefore, $j|n$.



- Note:
  - $\gamma^j V = V \Rightarrow \forall i, \gamma^{ji} V = V$.
  - $\left(\gamma^{ji_1} + \gamma^{ji_2}\right) V \subseteq \gamma^{ji_1} V + \gamma^{ji_2} V = V + V = V$
- Corollary 1: $\langle \gamma^j \rangle$ is a subfield. $\Rightarrow$ $|\langle \gamma^j \rangle| = q^t - 1, \ t|n$
- Corollary 2: $\bigcup_{i=0}^{j-1} \gamma^i \cdot \langle \gamma^j \rangle = \mathbb{F}_{q^n}^*$ $\Rightarrow$ $j(q^t - 1) = q^n - 1$

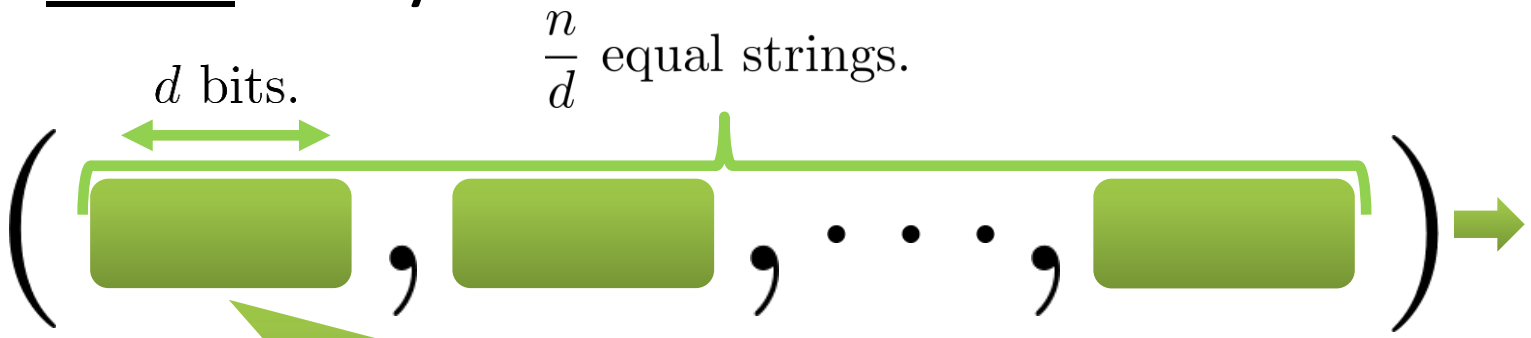
$$j = \frac{q^n - 1}{q^t - 1}$$

Degenerate Orbit - $t > 1$

Enumeration of Full-Length Necklaces

- Let $N(n,\varepsilon)$ be the number of n bit full-length necklaces, and Hamming weight εn.
  - Alternatively, $N(n,\varepsilon) = \frac{|\{b \in \{0,1\}^n : |Nec(b)| = n, w_H(b) = \varepsilon n\}|}{n}$.
- Lemma –
  - The number of n bit strings with weight εn and $|Nec(b)| = d$ is $N(d,\varepsilon)$.
- Proof – any such b has the form:

$N(n,\varepsilon) = ?$



1:1 correspondence between d bit strings with full-necklaces and n-bit strings with necklaces of size d.

Enumeration of Full-Length Necklaces

- Corollary –
  - The total number of n-bit strings of weight εn - $\binom{n}{\varepsilon n}$.
  - Each necklace is of size $d|n$.
  - Thus, $\binom{n}{\varepsilon n} = \sum_{d|n} dN(d,\varepsilon)$.
- Corollary –

$$N(n,\varepsilon) = \frac{1}{k}\sum_{d|k}\binom{d}{\varepsilon d}\mu\left(\frac{k}{d}\right)$$

Möbius Inversion Theorem –

- If $f(n) = \sum_{d|n} g(d)$, then $g(n) = \sum_{d|n} \mu(d) f(n/d)$
- Where

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^r & \text{if } n \text{ is a product of } r \text{ distinct primes} \\ 0 & \text{otherwise} \end{cases}$$

Enumeration of Full-Length Orbits

- Reminder – if $V \in \mathcal{G}_q(n,k)$, then $|Orb(V)| = \frac{q^n-1}{q^d-1}$ for some $d|n$.
- Fact – if $d|n$ then $\mathcal{G}_{q^d}(n/d, k/d) \overset{\varphi}{\hookrightarrow} \mathcal{G}_q(n,k)$.
- The image of φ is precisely the elements that are subspaces over $\mathbb{F}_{q^d}$ as well.
- Theorem: $|Orb(V)| = \frac{q^n-1}{q^d-1}$ iff $V \in \mathrm{Im}(\varphi)$, and $\varphi^{-1}(V)$ has a full-length orbit. (Note: $d|\gcd(n,k)$)
- Corollary: The number of orbits of length $\frac{q^n-1}{q^d-1}$ in $\mathcal{G}_q(n,k)$ equals to the number of full-orbits in $\mathcal{G}_{q^d}(n/d, k/d)$.

Enumeration of Full-Length Orbits

- Let $M_q(n,\varepsilon)$ be the number of full-length orbits in $\mathcal{G}_q(n,\varepsilon n)$.
  - Alternatively, $M_q(n,\varepsilon)=\dfrac{|\{V\in\mathcal{G}_q(n,\varepsilon n):|Orb(V)|=\frac{q^n-1}{q-1}\}|}{\frac{q^n-1}{q-1}}$.
- Corollary –

$$\begin{bmatrix} n \\ \varepsilon n \end{bmatrix}_q = \sum_{d|\gcd(n,\varepsilon n)} \frac{q^n-1}{q^d-1} M_{q^d}(n/d,\varepsilon)$$

$M_q(n,\varepsilon)=?$

Sum not over d|n…

Depends on n, not only on d…

- Möbius Inversion Theorem is *inapplicable*… ☹

Solution by [Drudge02]

- This problem was solved in “On the orbits of Singer groups and their subgroups” by Keldon Drudge, 2002.
- The number of orbits of size $\frac{q^n-1}{q^d-1}$ is

$$\frac{q^d-1}{q^n-1}\left(\sum_{t:d|t|\gcd(k,n)}\mu(t/d)\begin{bmatrix}n/t\\k/t\end{bmatrix}_{q^t}\right).$$

- Many thanks to Thomas Honold for the reference.

Thank you!