Duality of chains of almost affine codes

Diachkov Konstantin Aleksandrovich
Postgraduate
Northern (Arctic) Federal University named after M.V. Lomonosov

Abstract. Almost affine codes are generalization for widely used linear codes which can be used in ideal perfect secret sharing schemes. In [1] Simonis and Ashikhmin defined and studied some properties of almost affine codes. In the other hand quasi-uniform codes [2] are generalization of almost affine codes. In this paper we show that duality of chains of linear codes holds in the almost affine case as well and we make a conjecture about such property for quasi-uniform codes.

Keywords: almost affine codes, quasi-uniform codes, matroids.

Introduction

Linear block codes play a key role in the theory of error correction. A q-ary linear code of length n is a k-dimensional vector subspace of $\mathcal{F}_q^n$ where $\mathcal{F}$ is a finite field with q elements, also known as the alphabet of the code. One of the reasons why linear codes dominate the industry is that linear code can be described completely with its generator matrix. Because of the convenience, linear codes possess some restrictions, and it can be shown [9] that linear codes are not sufficient to achieve the maximal capacity for information flow in a multi-source network.

In [1] Simonis and Ashikhmin proposed another class of error correcting codes, namely almost affine codes. The initial motivation for authors was studying the ideal perfect secret sharing schemas. Basically, almost affine codes are generalization for linear codes with less restrictions. However, its turs out that almost affine codes share some properties with linear codes, like the subject of this paper – duality of chains of codes. Or specifically the demi-matroids associated with such chains.

The other step towards to generalization in error correction is quasi-uniform codes [3]. It can be shown that for small length ($n \leq 7$) almost affine codes are linear and, therefore satisfy the Ingleton inequality. But there is exists a quasi-uniform code of length equal to 4 which violates the Ingleton inequality.

We continue with giving formal definitions of concepts discussed earlier, starting with almost affine codes.

Definition 1. Let F be a finite set of cardinality q. A code $C \subseteq \mathrm{F}^{\mathrm{N}}$ is called almost affine if it satisfies the following condition for any subset $X \subseteq N$

$$r(X) := log_q(|C_X|) \in \mathbb{N}$$

As we can see F from the definition above does not have to be a field. And the condition says that projection to any subset of $[N] \coloneqq \{1, 2, \dots, n\}$ has an integer dimension. It is easy to verify that any linear code C satisfies this condition, therefore C is an almost affine code and r is called rank function of the code.

The main tool to study linear codes is their matrix representation. For almost affine codes we do not have such tool. But we have generalization of matrices – matroids. There are at least four equivalent definitions of matroids, we proceed with the definition via rank function.

Definition 2. Let E be a finite set called ground set, and r be a function $r: 2^E \mapsto \mathbb{N}$. Then matroid M is a pair (E, r) if r satisfies the following axioms for any $X \subseteq E$ and any $x, y \in E$

(R_1) $r(\emptyset) = 0$,

(R_2) $r(X) \leq r(X \cup \{x\}) \leq r(X) + 1$,

(R_3) If $r(X \cup \{x\}) = r(X \cup \{y\}) = r(X)$, then $r(X \cup \{x, y\}) = r(X)$.

It can be shown that the function from definition 1 satisfies the axioms above, and an almost affine code C induces a matroid. If r from definition above satisfies only (R_1) and (R_2) axioms, then a pair (E, r) is a demi-matroid. We continue with the core theorem of the article.

Theorem 1. Let $C_m \subset C_{m-1} \subset \cdots \subset C_1$ be a chain of almost affine codes with respective rank functions $r_m \leq r_{m-1} \leq \cdots \leq r_1$. Then (E, ρ_m) with $\rho_m = \sum_{i=1}^{m} (-1)^{i+1} r_i$ is a demi-matroid.

The prove of this theorem can be found in [6].

Demi-matroids have two types of duality. The dual demi-matroid to a given demi-matroid $M = (E, r)$ is $M^* = (E, r^*)$, where $r^*(X) \coloneqq r^*(X) = |X| + r(E \setminus X) - r(E)$. The supplement dual demi-matroid to a given one $M = (E, r)$ is $\overline{M} = (E, \overline{r})$, where $\overline{r}(X) \coloneqq r(E) - r(E \setminus X)$. It is known fact due to [10], that $M^* = (E, r^*)$, $\overline{M} = (E, \overline{r})$ and combination of the two types $\overline{M^*} = \left(E, \overline{r^*}\right)$ are demi-matroids.

Chains of almost affine codes

In this section we show that for any chain of almost affine codes $C_m \subset C_{m-1} \subset \cdots \subset C_1$ and rank functions $r_m \leq r_{m-1} \leq \cdots \leq r_1$ pairs (E, η_m), (E, θ_m) and (E, π_m) are also demi-matroids with

$$\eta_m \coloneqq r_m^* - r_{m-1}^* + \cdots + (-1)^{m+1} r_1^*$$

$$\theta_m \coloneqq \overline{r_1} - \overline{r_2} + \cdots + (-1)^{m+1} \overline{r_m}$$

$$\pi_m \coloneqq \overline{r_m^*} - \overline{r_{m-1}^*} + \cdots + (-1)^{m+1} \overline{r_1^*}$$

To do so we look at these three functions individually and show that under some circumstances they are equal to ρ^*, $\overline{\rho}$, $\overline{\rho^*}$ or just ρ.

Lemma 1. Let $C_m \subset C_{m-1} \subset \cdots \subset C_1$ be a chain of almost affine codes with respective rank functions $r_m \leq r_{m-1} \leq \cdots \leq r_1$ and $\rho_m \coloneqq r_1 - r_2 + \cdots + (-1)^{m+1} r_m$ and $\eta_m \coloneqq r_m^* - r_{m-1}^* + \cdots + (-1)^{m+1} r_1^*$. Then $\eta_m = \rho_m^*$ if m is odd and $\eta_m = \overline{\rho_m}$ if m is even.

Proof. For any $n \in \mathbb{N}_0$ we need to show

$$(*) \quad \begin{cases} \eta_{2n} = \overline{\rho_{2n}} \\ \eta_{2n+1} = \rho_{2n+1}^* \end{cases}$$

The equalities hold with $n = 0$. Assume (*) holds for any $i \leq n$, prove the induction step and show that $\eta_{2n+2} = \overline{\rho_{2n+2}}$ and $\eta_{2n+3} = \rho_{2n+3}^*$. By assumption we have $\eta_{2n+1} = \rho_{2n+1}^*$, notice that $\eta_{2n+2} = r_{2n+2}^* - \eta_{2n+1}$ by definition. Then $\eta_{2n+2} = r_{2n+2}^* - \rho_{2n+1}^*$, so by the definition of the dual we have:

$$\begin{aligned} \eta_{2n+2}(X) &= r_{2n+2}^*(X) - \rho_{2n+1}^*(X) \\ &= |X| + r_{2n+2}(E - X) - r_{2n+2}(E) - [|X| + \rho_{2n+1}(E - X) - \rho_{2n+1}(E)] = \\ &= (\rho_{2n+1} - r_{2n+2})(E) - (\rho_{2n+1} - r_{2n+2})(E - X) = \overline{\rho_{2n+2}}(X) \end{aligned}$$

Now we look at $\eta_{2n+3} = r_{2n+3}^* - \eta_{2n+2}$, combining with the above we have $\eta_{2n+3} = r_{2n+3}^* - \overline{\rho_{2n+2}}$, so by the definition of the supplement dual we have:

$$\begin{aligned} \eta_{2n+3}(X) &= r_{2n+3}^*(X) - \overline{\rho_{2n+2}}(X) \\ &= |X| + r_{2n+3}(E - X) - r_{2n+3}(E) - [\rho_{2n+2}(E) - \rho_{2n+2}(E - X)] = \\ &= |X| + (\rho_{2n+2} + r_{2n+3})(E - X) - (\rho_{2n+2} + r_{2n+3})(E) = \rho_{2n+3}^*(X). \end{aligned}$$

Thus, lemma is proven by induction.

Lemma 2. Let $C_m \subset C_{m-1} \subset \cdots \subset C_1$ be a chain of almost affine codes with respective rank functions $r_m \leq r_{m-1} \leq \cdots \leq r_1$ and $\rho_m \coloneqq r_1 - r_2 + \cdots + (-1)^{m+1} r_m$ and $\theta_m \coloneqq \overline{r_1} - \overline{r_2} + \cdots + (-1)^{m+1} \overline{r_m}$, then $\theta_m = \overline{\rho_m}$.

Proof.

$$\begin{aligned} \theta_m(X) &= \sum_{i=1}^{m} (-1)^{i+1} \overline{r_i} = \sum_{i=1}^{m} (-1)^{i+1} [r_i(E) - r_i(E \setminus X)] = \\ &= \sum_{i=1}^{m} (-1)^{i+1} r_i(E) - \sum_{i=1}^{m} (-1)^{i+1} r_i(E \setminus X) = \overline{\rho_m}(X) \end{aligned}$$

Before the last lemma we need the fact that $\forall X \subseteq E$ we have $\overline{r^*}(X) = (\overline{r})^*(X) = |X| - r(X)$. Indeed, by definition, we have

$$\overline{r^*}(X) = r^*(E) - r^*(E - X) = |E| + r(\emptyset) - r(E) - [|E| - |X| + r(X) - r(E)] = |X| - r(X)$$

At the same time, we have

$$(\bar{r})^*(X) = |X| + \bar{r}(E - X) - \bar{r}(E) = |X| + r(E) + r(X) - r(E) + r(\emptyset) = |X| - r(X).$$

Lemma 3. Let $C_m \subset C_{m-1} \subset \cdots \subset C_1$ be a chain of almost affine codes with respective rank functions $r_m \leq r_{m-1} \leq \cdots \leq r_1$ and $\rho_m := r_1 - r_2 + \cdots + (-1)^{m+1} r_m$ and $\pi_m := \overline{r_m^*} - \overline{r_{m-1}^*} + \cdots + (-1)^{m+1}\overline{r_1^*}$. Then $\pi_m = \rho_m$ if m is even and $\pi_m = \overline{\rho_m^*}$ if m is odd.

Proof. The proof is similar to the proof of lemma 1.

These three lemmas lead us to the following theorem.

Theorem 2. Let $C_m \subset C_{m-1} \subset \cdots \subset C_1$ be a chain of almost affine codes with respective rank functions $r_m \leq r_{m-1} \leq \cdots \leq r_1$, then the pairs (E, η_m), (E, θ_m) and (E, π_m) are demi-matroids.

Proof. By the theorem 1, $M = (E, \rho_m)$ is a demi-matroid, $M^* = (E, \rho_m^*)$, $\overline{M} = (E, \overline{\rho_m})$ and $\overline{M^*} = \left(E, \overline{\rho_m{}^*}\right)$ are demi-matroids as well. And by the previous lemmas we showed that the pairs (E, η_m), (E, θ_m) and (E, π_m) are equal to (E, ρ_m^*), $(E, \overline{\rho_m})$, $\left(E, \overline{\rho_m{}^*}\right)$ or (E, ρ_m) depending on the parity of m. Hence, the theorem is proven.

The theorem above is also proven in the article [6], but this prove is different. Applications of duality of chains of almost affine codes can be found in [6], [7] and [10].

Quasi-uniform codes

For proper introduction to quasi-uniform codes one can look at the article [3], where authors introduced these codes via random variable vectors. The simple recap is that quasi-uniform code $C \subseteq \mathrm{Z}^{|\mathrm{E}|}$ induces a random variable vector which is distributed uniformly over projection to any $X \subseteq E$. This class of codes does not have rank function r which can be used to construct its matroid. But quasi-uniform codes induce a polymatroids instead.

Definition 3. For a finite set E and h be a real value function $h : 2^E \mapsto \mathbb{R}$, then the pair (E, h) is a polymatroid if h for any $A, B \subseteq E$ satisfies the following axioms:

(R_1) $h(\emptyset) = 0$,

(R_2) $A \subseteq B \Rightarrow h(A) \leq h(B)$,

(R_3) $h(A \cup \mathrm{B}) + h(A \cap B) \leq h(A) + h(B)$.

If h satisfies cardinality bound $h(A) \leq |E|$ and $h(A)$ is a non-negative integer, then (E, h) is a matroid. If h from definition above satisfies only (R_1) and (R_2) axioms, then a pair (E, h) is a demi-polymatroid.

Any given quasi-uniform code C induces a polymatroid by defining $h(X) \coloneqq H(C_X)$, where $H(C_X)$ is the entropy function of the codeword random variable. We conjecture that the chain duality discussed in the previous section holds for chains of quasi-uniform codes with respective demi-polymatroids. Recently it was shown in [8] that similar chain duality holds for rank-metric codes with (n, m)-demi-polymatroids which are the special case of demi-polymatroids. However, the general case is still open.

References

1. *Simonis J. and A. Ashikhmin, "Almost Affine Codes." Designs, Code and Cryptography, pp. 179-197, (1998).*
2. *Chan, H. and R. Yeung. "A combinatorial approach to information inequalities." Information Theory and Networking Workshop (Cat. No.99EX371) (1999): 63-.*
3. *Chan, T., A. Grant and T. Britz. "Quasi-Uniform Codes and Their Applications." IEEE Transactions on Information Theory 59 (2013): 7915-7926.*
4. *Oxley, J.. "Matroid Theory (Oxford Graduate Texts in Mathematics)." (2006).*
5. *Lin, Shu and D. Costello. "Error control coding - fundamentals and applications." Prentice Hall computer applications in electrical engineering series (1983).*
6. *Johnsen, T. and Hugues Verdure. "Flags of almost affine codes." ArXiv abs/1704.02819 (2017): n. pag.*
7. *Johnsen, T. and Hugues Verdure. "Generalized Hamming Weights for Almost Affine Codes." IEEE Transactions on Information Theory 63 (2017): 1941-1953.*
8. *Ghorpade, S. and T. Johnsen. "A Polymatroid Approach to Generalized Weights of Rank Metric Codes." Des. Codes Cryptogr. 88 (2020): 2531-2546.*
9. *Chan, T. and A. Grant. "Dualities Between Entropy Functions and Network Codes." IEEE Transactions on Information Theory 54 (2008): 4470-4487.*
10. *Britz, T., T. Johnsen, D. Mayhew and K. Shiromoto. "Wei-type duality theorems for matroids." Designs, Codes and Cryptography 62 (2012): 331-341.*