Toric Codes, Multiplicative Structure and Decoding

Johan P. Hansen[1]

Department of Mathematics, Aarhus University

Abstract

Long linear codes constructed from toric varieties over finite fields, their multiplicative structure and decoding.

The main theme is the inherent multiplicative structure on toric codes. The multiplicative structure allows for *decoding*, resembling the decoding of Reed-Solomon codes and aligns with decoding by error correcting pairs.

We have used the multiplicative structure on toric codes to construct linear secret sharing schemes with *strong multiplication* via Massey's construction generalizing the Shamir Linear secret sharing shemes constructed from Reed-Solomon codes. We have constructed quantum error correcting codes from toric surfaces by the Calderbank-Shor-Steane method.

Keywords: Toric varieties, toric codes, decoding, error-correcting pairs, secret sharing
2010 MSC: 11H71, 11T71, 14M25, 14G50, 68P30, 94A60, 94A62, 98B35

1. Toric varieties and codes

In [1], [2] and [3] we introduced linear codes from toric varieties and estimated the minimum distance of such codes using intersection theory. Our method to estimate the minimum distance of toric codes has subsequently been supplemented, e.g., [4], [5], [6], [7], [8],[9] [10], and [11].

Toric codes have an inherent multiplicative structure.

We utilize the multiplicative structure to *decode* toric codes , resembling the decoding of Reed-Solomon codes and decoding by error correcting pairs,

Email address: matjph@math.au.dk (Johan P. Hansen)

[1]This work was supported by the Danish Council for Independent Research, grant no. DFF-4002-00367

see R. Pellikaan [12] , R. Kötter [13] and I. Márquez-Corbella and R. Pellikaan Ruud[14].

The multiplicative structure on toric codes gives rise to linear secret sharing schemes with the strong multiplication property. We presented this in [15] using the construction of J. L. Massey in [16] and [17, Section 4.1].

In [18] we used toric codes to construct quantum error correcting codes by the Calderbank-Shor-Steane method, see [19] and [20].

1.1. The construction of toric codes

Let $\square \subset \mathbb{R}^r$ be an integral convex polytope. Let $M \simeq \mathbb{Z}^r$ be the free $\mathbb{Z}$-module of rank r over the integers $\mathbb{Z}$. For $U = \square \cap M \subseteq M$, let $\mathbb{F}_q < U >$ be the linear span in $\mathbb{F}_q[X_1^{\pm 1}, \ldots, X_r^{\pm 1}]$ of the monomials

$$\{X^u = X_1^{u_1} \cdot \ldots \cdot X_r^{u_r} |\ u = (u_1, \ldots, u_r) \in U\} \ . \tag{1}$$

This is a $\mathbb{F}_q$-vector space of dimension equal to the number of elements in U.

Let $T(\mathbb{F}_q) = (\mathbb{F}_q^*)^r$ be the $\mathbb{F}_q$-rational points on the torus and let $S \subseteq T(\mathbb{F}_q)$ be any subset. The linear map that evaluates elements in $\mathbb{F}_q < U >$ at all the points in S is denoted by π_S:

$$\begin{array}{rcl} \pi_S : \mathbb{F}_q < U > & \to & \mathbb{F}_q^{|S|} \\ f & \mapsto & (f(P))_{P \in S} \ . \end{array}$$

In this notation $\pi_{\{P\}}(f) = f(P)$.

Evaluting at all points in the torus $T(\mathbb{F}_q)$, the *toric code* is obtained as the image $C = \pi_{T(\mathbb{F}_q)}(\mathbb{F}_q < U >) \subseteq \mathbb{F}_q^{|T(\mathbb{F}_q)|}$.

1.2. Multiplicative structure

Toric codes inherit a certain multiplicative structure, which we used in [15] to obtain LSSS with strong multiplication.

Let $\square$ and $\tilde{\square}$ be polyhedra in $\mathbb{R}^r$, let $\square + \tilde{\square}$ denote their Minkowski sum. Let $U = \square \cap \mathbb{Z}^r$ and $\tilde{U} = \tilde{\square} \cap \mathbb{Z}^r$. The map

$$\begin{array}{rcl} \mathbb{F}_q < U > \oplus \mathbb{F}_q < \tilde{U} > & \to & \mathbb{F}_q < U + \tilde{U} > \\ (f, g) & \mapsto & f \cdot g \ . \end{array}$$

induces a multiplication on the associated toric codes

$$\begin{array}{rcl} C_{\square} \oplus C_{\tilde{\square}} & \to & C_{\square + \tilde{\square}} \\ (c, \tilde{c}) & \mapsto & c \star \tilde{c} \end{array}$$

with coordinatewise multiplication of the codewords - the *Schur* product.

2. Multiplicative structure and decoding

Our goal is to use the multiplicative structure to correct t errors on the toric code $C_{\square}$.

This is achieved choosing another toric code $C_{\tilde{\square}}$ that helps to reduce error-correcting to a *linear* problem.

Let $\square$ and $\tilde{\square}$ be polyhedra as above in $\mathbb{R}^2$, let $\square + \tilde{\square}$ denote their Minkowski sum. Assume from now on:

i) $|\tilde{U}| > t$, where $\tilde{U} = \tilde{\square} \cap \mathbb{Z}^2$

ii) $d(C_{\square+\tilde{\square}}) > t$, where $d(C_{\square+\tilde{\square}})$ is the minimum distance of $C_{\square+\tilde{\square}}$.

iii) $d(C_{\tilde{\square}}) > n - d(C_{\square})$, where $d(C_{\square})$ and $d(C_{\tilde{\square}})$ are the minimum distances of $C_{\square}$ and $C_{\tilde{\square}}$.

2.1. Error-locating

Let the received word be $y(P) = f(P) + e(P)$ for $P \in T(\mathbb{F}_q)$, with $f \in \mathbb{F}_q < U >$ and error e of Hamming-weight at most t with support $T \subseteq T(\mathbb{F}_q)$, such that $|T| \leq t$.

From *i)*, it follows that there is a $g \in \mathbb{F}_q < \tilde{U} >$, such that $g_{|T} = 0$ - an *error-locator*. To find g, consider the linear map:

$$\mathbb{F}_q < \tilde{U} > \oplus \mathbb{F}_q < U + \tilde{U} > \ \rightarrow \ \mathbb{F}_q^n \tag{2}$$

$$(g, h) \ \mapsto \ (g(P)y(P) - h(P))_{P \in T(\mathbb{F}_q)} \tag{3}$$

As $y(P) - f(P) = 0$ for $P \notin T$ (recall that the support of the error e is T), we have that $g(P)y(P) - (g \cdot f)(P) = 0$ for all $P \in T(\mathbb{F}_q)$. That is $(g, h = g \cdot f)$ is in the kernel of (2).

Lemma 2.1. *Let (g, h) be in the kernel of (2). Then $g|T = 0$ and $h = g \cdot f$.*

Proof.

$$e(P) = y(P) - f(P) \quad \text{for} \quad P \in T(\mathbb{F}_q) \tag{4}$$

Coordinate wise multiplication yields by (2)

$$\begin{aligned} g(P)e(P) = & \ g(P)y(P) - g(P)f(P) \\ = & \ h(P) - g(P)f(P) \end{aligned}$$

for $P \in T(\mathbb{F}_q)$. The left hand side has Hamming weight at most t, the right hand side is a code word in $C_{\square+\tilde{\square}}$ with minimal distance strictly larger than t by assumption *ii)*. Therefore both sides equal 0. $\square$

2.2. Error-correcting

Lemma 2.2. *Let (g, h) be in the kernel of (2) with $g|T = 0$ and $g \neq 0$. There is a unique f such that $h = g \cdot f$.*

Proof. As in the above proof, we have

$$g(P)y(P) - g(P)f(P) = 0 \quad \text{for} \quad P \in T(\mathbb{F}_q) \tag{5}$$

Let $Z(g)$ be the zero-set of g with $T \subseteq Z(g)$. For $P \notin Z(g)$, we have $y(P) = f(P)$ and there are at least $d(C_{\tilde{\square}}) > n - d(C_{\square})$ such points by *iii)*. This determines f uniguely as it is determined by the values in $n - d(C_{\square})$ points. □

Example 2.3. Let $\square$ be the convex polytope with vertices $(0,0), (a,0)$ and $(0,a)$. Let $\tilde{\square}$ be the convex polytope with vertices $(0,0), (b,0)$ and $(0,b)$. Their Minkowski sum $\square + \tilde{\square}$ is the convex polytope with vertices $(0,0), (a+b,0)$ and $(0,a+b)$, see figure 1.

From [3, Theorem 1.3], we have that $n = (q-1)^2, |\tilde{\square}| = \frac{(b+1)(b+2)}{2}, d(C_{\square}) = (q-1)(q-1-a), d(C_{\tilde{\square}}) = (q-1)(q-1-b)$ and $d(C_{\square+\tilde{\square}}) = (q-1)(q-1-(a+b))$ for the associated codes over $\mathbb{F}_q$.

Let $q = 16, a = 4$ and $b = 8$. Then $n = 225, |\tilde{\square}| = 45, d(C_{\square}) = 165, d(C_{\tilde{\square}}) = 105$ and $d(C_{\square+\tilde{\square}}) = 45$.

As $d(C_{\tilde{\square}}) = 105 > 60 = n - d(C_{\square})$, the procedure corrects t errors with $t < \text{Min}\left\{d(C_{\square+\tilde{\square}}), |\tilde{\square}|\right\} = 45$.

2.3. Error correcting pairs

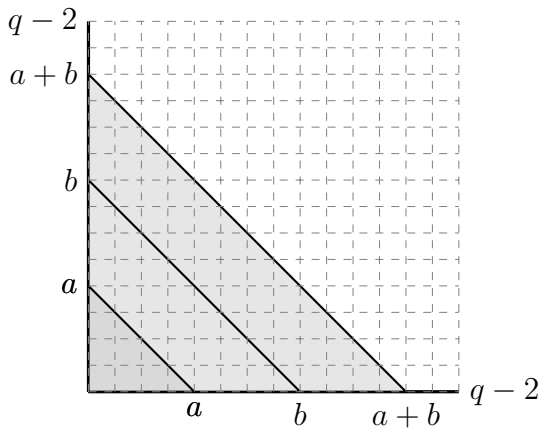
R. Pellikaan [12] and R. Kötter [13] introduced the concept of error correcting pairs for a linear code, see also I. Márquez-Corbella and R. Pellikaan Ruud[14]. Specifically for a linear code $C \subseteq \mathbb{F}_q^n$ an t-error correcting pair consists of two linear codes $A, B \subseteq \mathbb{F}_q^n$, such that

$$(A \star B) \perp C, \dim_{\mathbb{F}_q} A > t, d(B^{\perp}) > t, d(A) + d(C) > n \tag{6}$$

Here $A \star B = \{a \star b |\ a \in A, b \in B\}$ and $\perp$ denotes ortogonality with respect to the usual inner product. They described the known decoding algorithms for decoding t or fewer errors in this framwork.

Also the decoding in the present paper can be described in this framework, taking $C = C_{\square}, A = C_{\tilde{\square}}$ and $B = (C \star A)^{\perp}$ using Proposition 2.5.

Figure 1: The convex polytope $\square$ with vertices $(0,0),(a,0)$ and $(0,a)$. The convex polytope $\tilde{\square}$ with vertices $(0,0),(b,0)$ and $(0,b)$). Their Minkowski sum $\square + \tilde{\square}$ having vertices $(0,0),(a+b,0)$ and $(0,a+b)$.



2.3.1. Orthogonality - dual code

In Proposition 2.5 we present the dual code of $C = \pi_S(\mathbb{F}_q < U >)$.

Let $U \subseteq M$ be a subset, define its opposite as $-U := \{-u |\ u \in U\} \subseteq M$. The opposite maps the monomial X^u to X^{-u} and induces by linearity an isomorphism of vector spaces

$$\begin{array}{rcl} \mathbb{F}_q < U > & \to & \mathbb{F}_q < -U > \\ X^u & \mapsto & X^{-u} \\ f & \mapsto & \hat{f}\ . \end{array}$$

On $\mathbb{F}_q^{|T(\mathbb{F}_q)|}$, we have the usual inner product

$$(a_0, \ldots, a_n) \cdot (b_0, \ldots, b_n) = \sum_{l=0}^{n} a_l b_l \in \mathbb{F}_q\ , \tag{7}$$

with $n = |T(\mathbb{F}_q)| - 1$.

Lemma 2.4. *Let $f, g \in \mathbb{F}_q < M >$ and assume $f \neq \hat{g}$, then*

$$\pi_{T(\mathbb{F}_q)}(f) \cdot \pi_{T(\mathbb{F}_q)}(g) = 0 \tag{8}$$

Let

$$H = \{0, 1, \ldots, q-2\} \times \ldots \times \{0, 1, \ldots, q-2\} \subset M \ . \tag{9}$$

With this inner product we obtain the following proposition, e.g. [21, Proposition 3.5] and [22, Theorem 6].

Proposition 2.5. *Let $U \subseteq H$ be a subset. Then we have*

i) For $f \in \mathbb{F}_q < U >$ and $g \notin \mathbb{F}_q < -H \setminus -U >$, we have that $\pi_{T(\mathbb{F}_q)}(f) \cdot \pi_{T(\mathbb{F}_q)}(g) = 0$.

ii) The orthogonal complement to $\pi_{T(\mathbb{F}_q)}(\mathbb{F}_q < U >)$ in $\mathbb{F}_q^{|T(\mathbb{F}_q)|}$ is

$$\pi_{T(\mathbb{F}_q)}(\mathbb{F}_q < -H \setminus -U >) \ , \tag{10}$$

i.e., the dual code of $C = \pi_{T(\mathbb{F}_q)}(\mathbb{F}_q < U >)$ is $\pi_{T(\mathbb{F}_q)}(\mathbb{F}_q < -H \setminus -U >)$.

References

[1] J. Hansen, Toric surfaces and codes, in: Information Theory Workshop, IEEE, 1998, pp. 42–43. doi:10.1109/ITW.1998.706405.

[2] J. Hansen, Toric surfaces and error-correcting codes, in: J. Buchmann, T. Hoeholdt, H. Stichtenoth, H. Tapia-Recillas (Eds.), Coding theory, cryptography and related areas, Springer, 2000, pp. 132–142.

[3] J. Hansen, Toric varieties Hirzebruch surfaces and error-correcting codes, Applicable Algebra in Engineering, Communication and Computing 13 (4) (2002) 289–300.

[4] J. Little, H. Schenck, Toric surface codes and Minkowski sums, SIAM J. Discrete Math. 20 (4) (2006) 999–1014 (electronic). doi:10.1137/050637054.
URL `http://dx.doi.org/10.1137/050637054`

[5] I. Soprunov, J. Soprunova, Toric surface codes and Minkowski length of polygons, SIAM J. Discrete Math. 23 (1) (2008/09) 384–400. doi:10.1137/080716554.
URL `http://dx.doi.org/10.1137/080716554`

[6] J. Little, R. Schwarz, On toric codes and multivariate Vandermonde matrices, Appl. Algebra Engrg. Comm. Comput. 18 (4) (2007) 349–367. doi:10.1007/s00200-007-0041-1.

[7] D. Ruano, On the parameters of r-dimensional toric codes, Finite Fields Appl. 13 (4) (2007) 962–976. doi:10.1016/j.ffa.2007.02.002.
URL http://dx.doi.org/10.1016/j.ffa.2007.02.002

[8] P. Beelen, D. Ruano, The order bound for toric codes, in: M. Bras-Amors, T. Høholdt (Eds.), Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Vol. 5527 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2009, pp. 1–10.
URL http://dx.doi.org/10.1007/978-3-642-02181-7_1

[9] J. B. Little, Remarks on generalized toric codes, Finite Fields Appl. 24 (2013) 1–14. doi:10.1016/j.ffa.2013.05.004.
URL http://dx.doi.org/10.1016/j.ffa.2013.05.004

[10] I. Soprunov, Lattice polytopes in coding theory, J. Algebra Comb. Discrete Struct. Appl. 2 (2) (2015) 85–94. doi:10.13069/jacodesmath.75353.
URL http://dx.doi.org/10.13069/jacodesmath.75353

[11] J. B. Little, Toric codes and finite geometries, arxiv abs/1504.07494.
URL http://arxiv.org/abs/1504.07494

[12] R. Pellikaan, On decoding by error location and dependent sets of error positions, Discrete Math. 106/107 (1992) 369–381, a collection of contributions in honour of Jack van Lint.

[13] R. Kötter, A unified description of an error locating procedure for linear codes, in: Proceedings of Algebraic and Combinatorial Coding Theory, Voneshta Voda, 1992, pp. 113–117.

[14] I. Márquez-Corbella, R. Pellikaan, A characterization of MDS codes that have an error correcting pair, Finite Fields Appl. 40 (2016) 224–245. doi:10.1016/j.ffa.2016.04.004.
URL http://dx.doi.org/10.1016/j.ffa.2016.04.004

[15] J. P. Hansen, Secret Sharing Schemes with a large number of players from Toric Varieties, ArXiv e-printsarXiv:1410.4378.

[16] J. L. Massey, Some applications of code duality in cryptography, Mat. Contemp. 21 (2001) 187–209, 16th School of Algebra, Part II (Portuguese) (Brasília, 2000).

[17] H. Chen, R. Cramer, S. Goldwasser, R. de Haan, V. Vaikuntanathan, Secure computation from random error correcting codes, in: Advances in cryptology—EUROCRYPT 2007, Vol. 4515 of Lecture Notes in Comput. Sci., Springer, Berlin, 2007, pp. 291–310.

[18] J. P. Hansen, Quantum codes from toric surfaces, IEEE Trans. Inform. Theory 59 (2) (2013) 1188–1192. doi:10.1109/TIT.2012.2220523.
URL http://dx.doi.org/10.1109/TIT.2012.2220523

[19] A. Calderbank, P. Shor, Good quantum error-correcting codes exist, Physical Review A - Atomic, Molecular, and Optical Physics 54 (2) (1996) 1098–1105.

[20] A. Steane, Enlargement of calderbank-shor-steane quantum codes, IEEE Transactions on Information Theory 45 (7) (1999) 2492–2495.

[21] M. Bras-Amorós, M. E. O'Sullivan, Duality for some families of correction capability optimized evaluation codes, Adv. Math. Commun. 2 (1) (2008) 15–33. doi:10.3934/amc.2008.2.15.
URL http://dx.doi.org/10.3934/amc.2008.2.15

[22] D. Ruano, On the structure of generalized toric codes, J. Symbolic Comput. 44 (5) (2009) 499–506. doi:10.1016/j.jsc.2007.07.018.
URL http://dx.doi.org/10.1016/j.jsc.2007.07.018