# Some Optimal Codes as Tanner Codes with BCH Component Codes

Tom Høholdt, Fernando Piñero
Department of Applied Mathematics and Computer Science - DTU (Denmark)

Peng Zeng
Shanghai Key Laboratory of Trustworthy Computing – ECNU (China)

pzeng@sei.ecnu.edu.cn

**Abstract**

In this paper we study a class of graph codes with BCH component codes as affine variety codes. We are able to find some optimal binary and ternary codes as Tanner codes with BCH component codes. We choose a special subgraph of the point-line incidence plane of $\mathbb{P}(2,q)$ as the Tanner graph, and we are able to describe the codes using Gröbner basis.

**Keywords**
Tanner Graph, Tanner codes, graph codes, optimal codes

## Introduction

In 1981 Tanner [4] introduced a construction of error-correcting codes based on bipartite graphs. Since then results on their dimension, minimum distance and decoding have been obtained. In this paper we consider some specific bipartite graphs based on finite geometries and codes constructed from these graphs. We use techniques from algebra to compute the dimension when this class of graph codes has BCH component codes. We find some optimal binary and ternary codes in this class of codes.

In this paper $q$ denotes a power of prime $p$, $\mathbb{F}_q$ the field with $q$ elements, and $[n,k,d]_q$ a code with length $n$, dimension $k$, and minimum distance $d$ over $\mathbb{F}_q$.

## Tanner Codes and Graph Codes

In this section, we introduce two important codes based on graphs: Tanner Codes and Graph Codes. We also discuss the relations between the two constructions.

**Definition 1** ([4]). *Let $G$ be an $(m,n)$-regular bipartite graph with vertex set $V = V_1 \cup V_2$. Let $N = |V_1|$. For $v \in V_2$, we assume an ordering on the set $\mathcal{N}(v)$, the vertices in $V_1$ adjacent to $v$, given by $\phi_v$, where $\phi_v$ is a bijection from $\{1,2,\ldots,n\}$ to $\mathcal{N}(v)$. Furthermore we define $(c)_{\mathcal{N}(v)} := (c_{\phi_v(1)}, c_{\phi_v(2)}, \ldots, c_{\phi_v(n)}) \in \mathbb{F}_q^n$.*

*Let $C$ be a code of length $n$ over $\mathbb{F}_q$. We define the Tanner code*

$$(G,C) := \{(c_v) \in \mathbb{F}_q^N \mid \forall\ v \in V_2 :\ (c)_{\mathcal{N}(v)} \in C\}.$$

*The vertices of $V_1$ are known as the variable nodes, as they contain the symbols of the codewords. The vertices of $V_2$ are known as the constrain nodes, as they represent the parity check equations $(G,C)$ must satisfy.*

By using a highly structured graph, along with a highly structured code and well–chosen edge labelings, we describe the Tanner code in a nice, algebraic way. The importance of the labeling functions may not be clear from the definition, but the code parameters depend on them. We now define another class of graph based codes. For these codes the labeling functions $\phi_v$ play a fundamental role as well.

**Definition 2** ([3])**.** *Let $G$ be an $n$-regular bipartite graph with vertex set $V = V_1 \cup V_2$ and edge set $E$ of cardinality $\#E = N$. For $v \in V$, we assume an ordering on the set $E(v)$, the edges incident with $v$, given by $\phi_v$, where $\phi_v$ is a bijection from $\{1, 2, \ldots, n\}$ to $E(v)$. Furthermore we define $(c)_{E(v)} := (c_{\phi_v(1)}, c_{\phi_v(2)}, \ldots, c_{\phi_v(n)}) \in \mathbb{F}_q^n$.*

*Let $C_1$ and $C_2$ be codes of length $n$ over $\mathbb{F}_q$. We define the graph code*

$$(G, C_1 : C_2) := \{(c_e) \in \mathbb{F}_q^N \mid \forall\ v \in V_1 :\ (c)_{E(v)} \in C_1,\ \forall\ v \in V_2 :\ (c)_{E(v)} \in C_2\}.$$

Observe that

$$(G, C_1 : C_2) = (G, C_1 : \mathbb{F}_q^n) \cap (G, \mathbb{F}_q^n : C_2). \tag{1}$$

We define the vertex–edge incidence graph of $G$, which illustrates the close connection between Tanner codes and Graph codes.

**Definition 3.** *Let $G = (V(G), E(G))$ be a graph. We define the vertex-edge adjacency graph of $G$ as the bipartite graph $G_{ve} = (V(G) \cup E(G), E)$. There is an edge of the graph $G_{ve}$ between the vertex $v$ of $G$ and the edge $e$ of $G$ if and only if the vertex $v$ is incident to the edge $e$ in the graph $G$. $G_{ve}$ has no other edges.*

Now we state the close relation between Tanner Codes and Graph Codes.

**Theorem 1.** *Let $G$ be an $n$-regular bipartite graph. Let $C$ be a code of length $n$, then*

$$(G, [n, 1, n]_q : C) \text{ is an } n\text{-fold repetition of the code } (G, C) \text{ and } (G, C : C) = (G_{ve}, C).$$

*as long as the labelings are consistent.*

*Proof.* The equality $(G, C : C) = (G_{ve}, C)$ follows from the correspondence between the edges of $G$ and the vertices of $G_{ve}$. The equivalence between $(G, [n, 1, n] : C)$ and $(G, C)$ follows from the fact that since all edges incident to a vertex of $V_1$ must have the same value, we can assign this value to the vertex itself, which is the assignment for the code $(G, C)$. □

We finish this section with some theorems on the dimension of Graph codes.

**Theorem 2.** *Let $G$ be an $n$-regular bipartite graph with $N$ edges. Let $C_1$, $C_2$ be codes of length $n$ over $\mathbb{F}_q$ of dimensions $k_1$ and $k_2$ respectively. Then*

$$\dim\ (G, C_1 : C_2) = \frac{N}{n}(k_1 + k_2 - n) + \dim\ (G, C_1^\perp : C_2^\perp).$$

*Proof.* Assume $G$ has vertex set $V = V_1 \cup V_2$. For each vertex $v \in V_1$ we get $k_1$ independent parity check equations for $C_1^\perp$ involving the edges in $E(v)$ only. The resulting $Nk_1/n$ parity check equations of a code of the form $(G, C_1 : \mathbb{F}_q^n)$ are independent because the edge sets $E(v)$ and $E(u)$ are disjoint for $u \neq v$. Therefore the dimension of the code $(G, C_1^\perp : \mathbb{F}_q^n)$ is $N(n-k_1)/n$. Similarly, the code $(G, \mathbb{F}_q^n : C_2^\perp)$ has dimension $N(n-k_2)/n$. The parity check equations which are not independent are those corresponding to $(G, C_1^\perp : \mathbb{F}_q^n) \cap (G, \mathbb{F}_q^n : C_2^\perp)$ which are the codewords of $(G, C_1^\perp : C_2^\perp)$. □

The graph based codes in this paper are defined with the following graph.

**Definition 4.** *We define the bipartite graph* $\Gamma := (V_1 \cup V_2, E)$ *by:*

$$V_1 := \{(x, y) \mid x \in \mathbb{F}_q^*, y \in \mathbb{F}_q\},\ V_2 := \{(a, b) \mid a \in \mathbb{F}_q^*, b \in \mathbb{F}_q\}$$
$$\text{and } E := \{((x, y), (a, b)) \in V_1 \times V_2 \mid ax + b - y = 0\}.$$

Note that $\Gamma$ is a subgraph of the point line incidence graph of the projective plane over $\mathbb{F}_q$. Furthermore $\Gamma$ is $q-1$-regular and it has a nice algebraic description.

`Affine Variety Codes` We start this section with a review of material in [2] and [1]. Let $\mathbb{F}_q[X_1, \ldots, X_m]$ be the polynomial ring in $m$ variables over $\mathbb{F}_q$ and $\mathcal{P} = \{P_1, P_2, \ldots, P_N\} \subset \mathbb{F}_q^m$ be a set of $N$ points in $\mathbb{F}_q^m$. Denote by $\mathbf{I}(\mathcal{P})$ the ideal in $\mathbb{F}_q[X_1, \ldots, X_m]$ consisting of the polynomials which vanish at all points of $\mathcal{P}$. We define $R := \mathbb{F}_q[X_1, \ldots, X_m]/\mathbf{I}(\mathcal{P})$ and the evaluation map,

$$Ev_{\mathcal{P}} : R \quad \to \quad \mathbb{F}_q^N; \quad f \quad \mapsto \quad (f(P_1), f(P_2), \ldots, f(P_N)).$$

The map $Ev_{\mathcal{P}}$ is an isomorphism of vector spaces. Note that in this paper, we often denote an element $\bar{f} = f + \mathbf{I}(\mathcal{P}) \in R$ by $f$ for simplicity.

**Definition 5.** *Let* $L$ *be an* $\mathbb{F}_q$*-linear subspace of* $R$*. We define the* affine variety code $C(\mathbf{I}(\mathcal{P}), L) := Ev_{\mathcal{P}}(L)$.

Since $L$ is an $\mathbb{F}_q$-linear subspace of $R$ and $Ev_{\mathcal{P}}$ is an isomorphism, we have that

$$\dim C(\mathbf{I}(\mathcal{P}), L) = \dim L. \tag{2}$$

**Lemma 1.** *Let* $\mathcal{P} \subset \mathbb{F}_q^m$, $R = \mathbb{F}_q[X_1, X_2, \ldots, X_m]/\mathbf{I}(\mathcal{P})$ *as before. Suppose that* $L$ *and* $M$ *are two* $\mathbb{F}_q$*-linear subspaces of* $R$*. Then* $C(\mathbf{I}(\mathcal{P}), L) \cap C(\mathbf{I}(\mathcal{P}), M) = C(\mathbf{I}(\mathcal{P}), L \cap M)$.

*Proof.* If $c \in C(\mathbf{I}(\mathcal{P}), L) \cap C(\mathbf{I}(\mathcal{P}), M)$, then $f \in L$ and $g \in M$ exist such that $Ev_{\mathcal{P}}(f) = c = Ev_{\mathcal{P}}(g)$. Since $Ev_{\mathcal{P}}$ is injective, then $f = g$ and therefore that $f \in L \cap M$. Therefore $c \in C(\mathbf{I}(\mathcal{P}), L \cap M)$. The inclusion $C(\mathbf{I}(\mathcal{P}), L) \cap C(\mathbf{I}(\mathcal{P}), M) \supseteq C(\mathbf{I}(\mathcal{P}), L \cap M)$ is clear. □

Since the quotient ring $R$ plays a fundamental role on Affine Variety codes, the following theorem on an ideal $\mathbf{I}(\mathcal{P})$ and its quotient ring $R$ will help our computations with $R$.

**Theorem 3** ([1])**.** *Let* $\mathbf{I}(\mathcal{P})$ *be an ideal of* $\mathbb{F}_q[X_1, \ldots, X_m]$ *and* $R = \mathbb{F}_q[X_1, \ldots, X_m]/\mathbf{I}(\mathcal{P})$ *be the quotient ring of* $R$*. Let* $\delta$ *be a monomial ordering, and suppose* $\{g_1, g_2, \ldots, g_{m'}\}$ *is a Gröbner basis for* $\mathbf{I}(\mathcal{P})$ *under* $\delta$ *and let* $\Delta_\delta$ *be the set of monomials which are not divisible by the leading terms of the* $g_i$ *under* $\delta$*. Then the following are true:*

- $\Delta_\delta$*, also known as the footprint of* $\mathbf{I}(\mathcal{P})$ *under* $\delta$*, is a* $\mathbb{F}_q$*-linear basis for* $R$*.*
- *The representation of* $f \in R$ *over* $\Delta_\delta$ *is* $f \mod \{g_1, g_2, \ldots, g_{m'}\}$ *.*

BCH codes are an example of affine variety codes with $m = 1$ and $\mathcal{P} = \{\alpha_1, \alpha_2, \ldots, \alpha_{q-1}\} = \mathbb{F}_q^*$. Then $\mathbf{I}(\mathcal{P}) = \langle X_1^{q-1} - 1 \rangle$. BCH codes have several definitions; we use the following. Let $q$ be a power of $p$. Let $J \subseteq \mathbb{Z}_{q-1}$, such that $J$ is closed under multiplication by $p$ modulo $q-1$. We define $M(J) := \langle \{X_1^j \mid j \in J\} \rangle_{\mathbb{F}_q}$ of $R = \mathbb{F}_q[X_1]/\mathbf{I}(\mathcal{P})$. The BCH code is the affine variety code $C(\mathbf{I}(\mathcal{P}), M(J))$. The $i$-th coordinate of $Ev_{\mathcal{P}}(f)$ is $f(\alpha_i)$. Furthermore if we define $\bar{J} = \{q - 1 - j \mod (q-1) \mid j \in J\}$ for $J \subset \mathbb{Z}_{q-1}$, then $C(\mathbf{I}(\mathcal{P}), M(J))^\perp = C(\mathbf{I}(\mathcal{P}), M(\mathbb{Z}_{q-1} \setminus \bar{J}))$. The theory of subfield subcodes ensures that this definition is equivalent to the standard definitions of BCH codes.

Now we describe Graph codes over $\Gamma$ as Affine Variety codes. Since a Graph code over $G$ assigns a symbol from $\mathbb{F}_q$ to each edge in $E(G)$, we must associate a polynomial ideal $I(\Gamma)$ to the edge set $E = E(\Gamma)$. To do this, let $\delta_1$ denote the lexicographical order with $B > A > X > Y$ and $\delta_2$ denote the lexicographical order with $Y > X > A > B$, we have the following theorem for the ideal $\mathbf{I}(\Gamma) := \langle AX + B - Y, X^{q-1} - 1, Y^q - Y, A^{q-1} - 1, B^q - B \rangle$.

**Theorem 4.** *The set* $\{AX+B-Y, X^{q-1}-1, Y^q-Y, A^{q-1}-1, B^q-B\}$ *is a Gröbner basis for* $\mathbf{I}(\Gamma)$ *under* $\delta_1$ *and* $\delta_2$.

*Proof.* The polynomial $B^q-B$ is a combination of the other four polynomials, $AX+B-Y, X^{q-1}-1, Y^q-Y, A^{q-1}-1$. As no leading term under $\delta_1$ of this basis for $\mathbf{I}(\Gamma)$ contains any common factor with another leading term, these four polynomials constitute a Gröbner basis for $\mathbf{I}(\Gamma)$. The proof for $\delta_2$ is similar. □

Denote by $\Delta_1$ the footprint of $\mathbf{I}(\Gamma)$ under $\delta_1$ and by $\Delta_2$ the footprint of $\mathbf{I}(\Gamma)$ under $\delta_2$.

**Theorem 5.** *The ideal* $\mathbf{I}(\Gamma)$ *is the ideal of* $E$*, the edge set of* $\Gamma$.

*Proof.* The elements of $\mathbf{I}(\Gamma)$ vanish at all the points of $E$. Therefore $\mathbf{I}(\Gamma) \subset \mathbf{I}(E)$. This implies that $\dim \mathbb{F}_q[X,Y,A,B]/\mathbf{I}(\Gamma) \geq \dim \mathbb{F}_q[X,Y,A,B]/\mathbf{I}(E) = \#E = q(q-1)^2$. Since $\#\Delta_1 = q(q-1)^2$, then $\dim \mathbb{F}_q[X,Y,A,B]/\mathbf{I}(\Gamma) = q(q-1)^2$, which implies $\mathbf{I}(\Gamma) = \mathbf{I}(E)$ □

We need a vertexwise edge labeling of the edges of $\Gamma$. The labelings we will use are:

$$\phi_{(x,y)}(i) := (x, y, \alpha_i, y - x\alpha_i), \quad (x,y) \in V_1, \text{ and } \phi_{(a,b)}(i) := (\alpha_i, a\alpha_i + b, a, b), \quad (a,b) \in V_2.$$

For any $J \subset \mathbb{Z}_{q-1}$, we describe the codes $(\Gamma, C(\mathbf{I}(\mathcal{P}), M(J)) : \mathbb{F}_q^{q-1})$ and $(\Gamma, \mathbb{F}_q^{q-1} : C(\mathbf{I}(\mathcal{P}), M(J)))$ as affine variety codes.

**Definition 6.** *Let* $J \subset \mathbb{Z}_{q-1}$ *and* $R = \mathbb{F}_q[X,Y,A,B]/\mathbf{I}(\Gamma)$*, we define*

$$L_1(J) := \langle \{X^{i_1} Y^{i_2} A^{j_1} \mid j_1 \in J\} \rangle_{\mathbb{F}_q} \subset R, \text{ and } L_2(J) := \langle \{A^{j_1} B^{j_2} X^{i_1} \mid i_1 \in J\} \rangle_{\mathbb{F}_q} \subset R.$$

Note that the elements of $L_1(J)$ and $L_2(J)$ belong to the quotient ring $R$. In particular the monomials in the above definition may not be linearly independent, because we are working modulo $\mathbf{I}(\Gamma)$. We use the representations of $L_1(J_X)$ and $L_2(J_A)$ under $\Delta_1$ and $\Delta_2$ to describe the graph code $(\Gamma, C(\mathbf{I}(\mathcal{P}), M(J_X)) : C(\mathbf{I}(\mathcal{P}), M(J_A)))$ as an affine variety code. By Eq. (1) we have the equality $(\Gamma, C(\mathbf{I}(\mathcal{P}), M(J_X)) : C(\mathbf{I}(\mathcal{P}), M(J_A))) = (\Gamma, C(\mathbf{I}(\mathcal{P}), M(J_X)) : \mathbb{F}_q^{q-1}) \cap (\Gamma, \mathbb{F}_q^{q-1} : C(\mathbf{I}(\mathcal{P}), M(J_A)))$.

**Theorem 6.** *We have*

$$C(\mathbf{I}(\Gamma), L_1(J_X)) = (\Gamma, C(\mathbf{I}(\mathcal{P}), M(J_X)) : \mathbb{F}_q^{q-1})$$

$$\text{and } C(\mathbf{I}(\Gamma), L_2(J_A)) = (\Gamma, \mathbb{F}_q^{q-1} : C(\mathbf{I}(\mathcal{P}), M(J_A))).$$

$$\text{Moreover, } (\Gamma, C(\mathbf{I}(\mathcal{P}), M(J_X)) : C(\mathbf{I}(\mathcal{P}), M(J_A))) = C(\mathbf{I}(\Gamma), L_1(J_X) \cap L_2(J_A)).$$

*Proof.* Let $f(X,Y,A,B) \in L_1(J_X)$ and $c = (f(x,y,a,b))_{(x,y,a,b)\in E}$. For $(x,y) \in V_1$, the univariate polynomial $p(A) := f(x,y,A,y-Ax)$ is in the vector space $\langle \{A^j \mid j \in J_X\} \rangle_{\mathbb{F}_q}$ since the coefficients where $y - Ax$ is raised to a nonzero power are zero . Therefore the codeword $(p(\alpha_1), p(\alpha_2), \ldots, p(\alpha_{q-1}))$ is a codeword in $C(\mathbf{I}(\mathcal{P}), M(J_X))$. On the other hand $(c)_{E((x,y))} = (f(x,y,\alpha_1, y-\alpha_1 x), \ldots, f(x,y,\alpha_{q-1}, y-\alpha_{q-1}x))$. We see that the value of the polynomial $p(A)$ at $A = \alpha_i$ is equal to the $i$-th coordinate of $(c)_{E((x,y))}$. Therefore $c \in (\Gamma, C(\mathbf{I}(\mathcal{P}), M(J_X)) : \mathbb{F}_q^{q-1})$ implying $C(\mathbf{I}(\Gamma), L_1(J_X)) \subset (\Gamma, C(\mathbf{I}(\mathcal{P}), M(J_X)) : \mathbb{F}_q^{q-1})$.

By the reasoning in the proof of Theorem 2, we obtain $\dim(\Gamma, C(\mathbf{I}(\mathcal{P}), M(J_X)) : \mathbb{F}_q^{q-1}) = q(q-1)|J_X|$. Since the elements of $L_1(J_X) \cap \Delta_1$ are linearly independent, the inequality $\dim L_1(J_X) \geq q(q-1)|J_X| = |L_1(J_X) \cap \Delta_1|$ follows easily. Equation (2), implies $C(\mathbf{I}(\Gamma), L_1(J_X)) = (\Gamma, C(\mathbf{I}(\mathcal{P}), M(J_X)) : \mathbb{F}_q^{q-1})$. Similarly $C(\mathbf{I}(\Gamma), L_2(J_A)) = (\Gamma, \mathbb{F}_q^{q-1} : C(\mathbf{I}(\mathcal{P}), M(J_A)))$ holds. The final statement follows from the above and Lemma 1. □

The dimension of $(\Gamma, C(\mathbf{I}(\mathcal{P}), M(J_X)) : C(\mathbf{I}(\mathcal{P}), M(J_A)))$ equals the dimension of the $\mathbb{F}_q$-linear subspace $\langle L_1(J_X)\rangle_{\mathbb{F}_q} \cap \langle L_2(J_A)\rangle_{\mathbb{F}_q}$ of $R$ . Although $L_1(J_X) \cap \Delta_1$ is a basis for $\langle L_1(J_X)\rangle_{\mathbb{F}_q})$ and $L_2(J_A) \cap \Delta_2$ is a basis for $\langle L_2(J_A)\rangle_{\mathbb{F}_q}$, their intersection is hard to compute. Since the Gröbner basis for $I(\Gamma)$ under $\delta_1$ is nice, the remainder of $f \in \langle \Delta_2 \rangle$ over the basis $\Delta_1$ is also nice, wihch implies the change of basis matrix from $\Delta_2$ to $\Delta_1$ is quite nice.

**Theorem 7.** *Let $U_q = (\binom{j}{i})_{0 \le i,j < q}$ be the upper triangular Pascal matrix of binomial coefficients in $\mathbb{F}_p$. Then the change of basis matrix from $\Delta_1$ to in $\Delta_2$ is a permutation of a block diagonal $q(q-1)^2 \times q(q-1)^2$ matrix with $(q-1)^2$ blocks of the matrix $U_q$.*

*Proof.* Fix $0 \le i_1, j_1 < q-1$. A monomial of the form $X^{i_1-l}A^{j_1-l}Y^l$, where the powers $i_1 - l$ and $j_1 - l$ are taken $\mod q-1$ is mapped to $\Sigma_{m=0}^{l}\binom{l}{m}B^m A^{j_1-m}X^{i_1-m}$. Therefore a polynomial in $\langle X^{i_1-l}A^{j_1-l}Y^l\rangle_{\mathbb{F}_q}$ is mapped to a polynomial in $\langle X^{i_1-l}A^{j_1-l}B^l\rangle_{\mathbb{F}_q}$ according to the Pascal matrix $U_q$. □

With this simpler basis, we can easily compute the dimension of the $\mathbb{F}_q$-linear space $L_1(\{0\}), \cap L_2(J_A)$. We present some optimal codes we have found in this manner.

`Optimal Codes`

We have found some optimal binary and ternary codes as Tanner codes of the graph $\Gamma$ with the BCH component codes described in the following table.

| $q$ | $J_A$ | $(\Gamma, C(\mathbf{I}(\mathcal{P}), M(J_A)))$ | Status |
|---|---|---|---|
| 8 | $\{1,2,4\}$ | $[56,6,28]_2$ | Optimal |
| | $\{0,1,2,4\}$ | $[56,10,24]_2$ | Optimal |
| 16 | $\{5,10\}$ | $[240,2,160]_2$ | Optimal |
| | $\{1,2,4,8\}$ | $[240,8,120]_2$ | Optimal |
| | $\{0,1,2,4,8\}$ | $[240,13,112]_2$ | Best Known |
| 9 | $\{1,3\}$ | $[72,2,54]_3$ | Optimal |
| | $\{0,1,3\}$ | $[72,5,45]_3$ | Best Known |

`Acknowledgment` The authors gratefully acknowledge the support from the Danish National Research Foundation and the National Science Foundation of China (Grant No.11061130539) for the Danish-Chinese Center for Applications of Algebraic Geometry in Coding Theory and Cryptography. The third author would also like to acknowledge the support of the National Natural Science Foundation of China under Grants No. 61021004 and 61103222 and the Research Fund for the Doctoral Program of Higher Education of China under grant No. 20110076120016.

# References

[1] David Cox, John Little, and Donal O'Shea. *Ideals, Varieties and Algorithms.* Springer, 2007.

[2] J. Fitzgerald and R.F. Lax. Decoding affine variety codes using Gröbner bases. *DCC*, 13:147–158, 1998.

[3] Ron M. Roth. *Introduction to Coding Theory.* Cambridge University Press, 2006.

[4] R. Tanner. A recursive approach to low complexity codes. *IEEE Trans. Inf. Theory*, 27(5):533 – 547, sep 1981.