Rose-Hulman Undergraduate Mathematics Journal

Volume 14
Issue 2

Article 10

Entanglement-Assisted Quantum Error-Correcting Codes from Generalized Quadrangles

William Thomas
University of Chicago, wcthomas@uchicago.edu

Follow this and additional works at: https://scholar.rose-hulman.edu/rhumj

Recommended Citation
Thomas, William (2013) "Entanglement-Assisted Quantum Error-Correcting Codes from Generalized Quadrangles," *Rose-Hulman Undergraduate Mathematics Journal*: Vol. 14 : Iss. 2 , Article 10.
Available at: https://scholar.rose-hulman.edu/rhumj/vol14/iss2/10

Rose-
Hulman
Undergraduate
Mathematics
Journal

Entanglement-Assisted Quantum Error-Correcting Codes from Generalized Quadrangles

William Thomas[a]

Volume 14, no. 2, Fall 2013

Sponsored by

Rose-Hulman Institute of Technology
Department of Mathematics
Terre Haute, IN 47803
Email: mathjournal@rose-hulman.edu
http://www.rose-hulman.edu/mathjournal

[a]University of Chicago, email: wcthomas@uchicago.edu

Rose-Hulman Undergraduate Mathematics Journal
Volume 14, no. 2, Fall 2013

Entanglement-Assisted Quantum Error-Correcting Codes from Generalized Quadrangles

William Thomas

Abstract. A generalized quadrangle GQ(s,t) is an incidence structure consisting of points and lines in which each line is incident with a fixed number of points, each point is incident with a fixed number of lines, and there is exactly one line connecting any point with a line not incident with the point. Entanglement-assisted quantum error-correcting codes provide a method for correcting data transmission errors in quantum computers. EAQECCs require entangled quantum states, called ebits, and it is desirable to minimize the number of ebits a code uses because ebits are difficult to manufacture. We use a binary incidence matrix N of a generalized quadrangle to create entanglement-assisted quantum error-correcting codes. The rank of NN^T gives the number of ebits a code requires. Because incidence matrices of generalized quadrangles are highly structured and reflect the geometric properties of the quadrangles, we can examine the rank of N and NN^T and write the parameters of quantum codes in terms of s and t. We identify a class of generalized quadrangles that produce quantum codes that require a low number of ebits, a class that produce quantum codes that require a large number of ebits, and a class that produces quantum codes that are too small to be useful.

Acknowledgements: I would like to sincerely thank Dr. David Clark for all of his help as my advisor for this project, and I would like to thank the University of Minnesota Math Center for Educational Programs for funding my trip to present my results at a Pi Mu Epsilon conference. I am also very grateful for the anonymous referee's feedback.

1 Introduction

Quantum computers are a recently developed class of machines that would perform computations by taking advantage of quantum mechanical principles. The units of data in a quantum computer are called qubits and are analogous to bits in a digital computer. In any computer, errors occur during data transmission. Quantum computers are especially prone to errors because of the effects of quantum mechanics. Luckily, by encoding data in a certain way, many of these errors can be corrected. An entanglement-assisted quantum error-correcting code is a method for correcting errors in data transmission in quantum computers. We will not cover the details of the physics here, but physicists have shown that quantum codes can be created using entangled quantum states, or ebits [2]. Ebits are related to the "spooky action at a distance" described by Einstein as a consequence of quantum mechanics. An $[[n, k; c]]$ entanglement-assisted quantum error-correcting code encodes k logical qubits as n physical qubits using c ebits. In other words, the code takes k qubits of data and encodes them as n qubits of data, which are then transmitted and decoded. Consequently, an $[[n, k; c]]$ quantum code has codewords of length n in a linear space of dimension k and requires c ebits.

A surprising link between EAQECCs and binary matrices is proved in [2]: An EAQECC can be defined by a binary matrix N, and $\text{rank}_2(NN^T)$ is the number of ebits the code uses, where $\text{rank}_2(NN^T)$ denotes the binary rank of NN^T. Note that when multiplying binary matrices we set $1+1 = 0$ and perform all other arithmetic normally. Therefore, $\text{rank}_2(NN^T)$ is the rank of a binary matrix computed the usual way but with the rule that $1 + 1 = 0$.

Ebits are difficult to manufacture, so we are interested in minimizing $\text{rank}_2(NN^T)$. To do this, we will look for highly structured binary matrices. These are provided by a geometric structure called generalized quadrangles, whose incidence matrices reflect their geometric structure. We will examine $\text{rank}_2(NN^T)$ when N is the incidence matrix of a generalized quadrangle, and we will create some quantum codes from generalized quadrangles.

In Section 2 we provide the necessary background concerning generalized quadrangles and quantum codes. In Section 3 we calculate $\text{rank}_2(NN^T)$ for some special types of generalized quadrangles, which we use in Section 4 to provide some examples of quantum codes from generalized quadrangles. Finally, in Section 5 we provide some concluding remarks.

2 Background

A generalized quadrangle $\text{GQ}(s, t)$ is a finite set of lines and points defined by the following three properties:

1. Each point is incident with $t + 1$ lines, and two distinct points are incident with at most 1 line.

2. Each line is incident with $s + 1$ points, and two distinct lines are incident with at most 1 point.

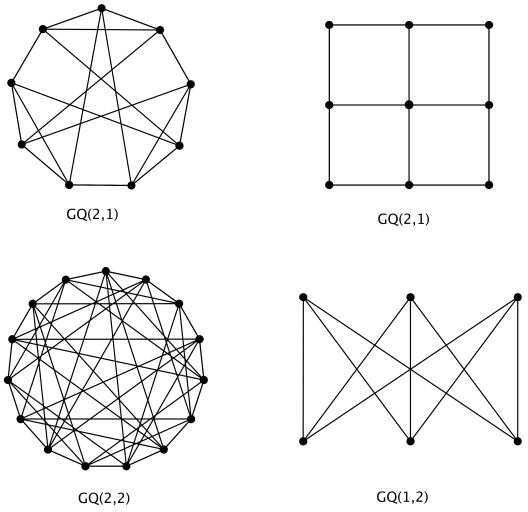

Figure 1: Generalized Quadrangles

3. If x is a point and L is a line not incident with x, then there is exactly one line through x that shares a point with L.

Some examples of generalized quadrangles are shown in Figure 1. The "lines" of the two generalized quadrangless on the left are represented by triangles, while the lines of the two on the right are represented by line segments. The top two are different representations of the same generalized quadrangle, $\mathrm{GQ}(2,1)$. The name "generalized quadrangles" reflects the fact that generalized quadrangles are triangle-free in the sense that no three lines of a generalized quadrangle form a triangle; that is, there is no set of three lines such that each intersects the other two (though the lines themselves might be represented as triangles, as in $\mathrm{GQ}(2,1)$ in the upper left corner of Figure 1).

The line-by-point incidence matrix N of a generalized quadrangle is the matrix such that

$$N_{ij} = \begin{cases} 1 & \text{if the } i\text{th line is incident with the } j\text{th point,} \\ 0 & \text{otherwise.} \end{cases}$$

Example 1. *The line-by-point incidence matrix of* $\mathrm{GQ}(2,1)$ *is*

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

A generalized quadrangle $\mathrm{GQ}(s,t)$ has $(s+1)(st+1)$ points and $(t+1)(st+1)$ lines, so its line-by-point incidence matrix N has dimensions $(t+1)(st+1) \times (s+1)(st+1)$. For more information about generalized quadrangles, see [3].

We are going to use incidence matrices of generalized quadrangles to create quantum error-correcting codes. Recall that the parameters $[[n,k;c]]$ describe a quantum code, and we want to minimize c, the number of ebits the code uses. The following proposition will allow us to use generalized quadrangles to create quantum codes.

Proposition 1 (Brun, Devetak, Hsieh [2])**.** *Let H be a block-by-point incidence matrix of an incidence structure (V,B). Then there exists an EAQECC with parameters*

$$[[|V|, |V| - 2\operatorname{rank}_2 H + \operatorname{rank}_2 HH^T; \operatorname{rank}_2 HH^T]].$$

Therefore, if the line-by-point incidence matrix N of a generalized quadrangle is $m \times n$, then there exists a quantum code with parameters

$$[[n, n - 2\operatorname{rank}_2(N) + \operatorname{rank}_2(NN^T); \operatorname{rank}_2(NN^T)]].$$

For more information about Entanglement Assisted QECCs, see [2].

Using Proposition 1 and the number of points in a generalized quadrangle, a line-by-point incidence matrix of a generalized quadrangle defines a

$$[[(s+1)(st+1), (s+1)(st+1) - 2\operatorname{rank}_2(N) + \operatorname{rank}_2(NN^T); \operatorname{rank}_2(NN^T)]]$$

quantum code.

3 Results

We will determine $\operatorname{rank}_2(NN^T)$ for certain generalized quadrangles in order to determine the number of ebits needed by quantum codes defined by the line-by-point incidence matrices of those generalized quadrangles.

3.1 $\mathrm{GQ}(s,1)$

We first consider generalized quadrangles with $t = 1$ and s odd. Let N be a line-by-point incidence matrix of $\mathrm{GQ}(s,1)$. Note that $\mathrm{GQ}(s,1)$ has $2(s+1)$ lines and $(s+1)^2$ points, so N is $2(s+1) \times (s+1)^2$ and NN^T is $2(s+1) \times 2(s+1)$.

Lemma 1. *Let l_i be the ith line of $\mathrm{GQ}(s,t)$. If $|l_i \cap l_j|$ is odd, then the ijth entry of NN^T is 1. Otherwise, the ijth entry is 0.*

Proof. Let $NN^T = (n_{ij})$. Then n_{ij} is the dot product of the ith row of N and the jth column of N^T, which is the same as the jth row of N. As a reminder, all of our calculations are binary. Therefore, since the rows of N represent lines of $\mathrm{GQ}(s,t)$, the dot product of the ith and jth rows of N is 1 if $|l_i \cap l_j|$ is odd and 0 if $|l_i \cap l_j|$ is even. □

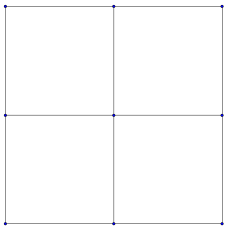

Figure 2: GQ$(2,1)$

This lemma allows us to identify $\text{rank}_2(NN^T)$ for GQ$(s,1)$.

Theorem 1. *Let N be the line-by-point incidence matrix of* GQ$(s,1)$*. If s is odd, then* $\text{rank}_2(NN^T) = 2$*.*

Proof. Since each line in GQ$(s,1)$ is incident with $s+1$ points, each line is incident with an even number of points if s is odd. This means that each line shares an even number of points with itself, so the diagonal of NN^T is all zeroes by Lemma 1.

Each line l of GQ$(s,1)$ is incident with $s+1$ points. Since each point of l is incident with 2 lines (one of which is l), each line of GQ$(s,1)$ intersects $s+1$ other lines. These lines must be distinct; otherwise, two points would be on the same line. These $s+1$ lines are parallel to each other because if they were not, the point where any two of them intersect would be incident with two distinct lines that intersect l. This would violate the third part of the definition of a generalized quadrangle. GQ$(s,1)$ has $2(s+1)$ lines, so there must be $2(s+1)-(s+1) = s+1$ lines parallel to a given line. This means that the lines of GQ$(s,1)$ can be divided into two parallel classes each containing $s+1$ lines. Visually, this means that GQ$(s,1)$ can be drawn as a grid like the one shown in Figure 2.

We will write N so that the first $s+1$ rows correspond to lines belonging to the first parallel class and the last $s+1$ rows correspond to lines belonging to the second parallel class. Lines in the same parallel class share no points, so the dot product of two rows in the first $s+1$ rows or two lines in the last $s+1$ rows is 0 by Lemma 1. In a generalized quadrangle, two lines can share at most one point. Therefore, the dot product of two rows representing lines not in the same parallel class is 1. As a result, NN^T has two blocks of zeroes on the diagonal and ones everywhere else. That is,

$$NN^T = \left[\begin{array}{c|c} 0 & J \\ \hline J & 0 \end{array}\right],$$

where J is the $(s+1)\times(s+1)$ matrix of all ones.

This means that the first $s+1$ of the $2(s+1)$ rows of NN^T are identical, and the other $s+1$ rows are identical to each other and linearly independent of the first $s+1$ rows. Thus $\text{rank}_2(NN^T) = 2$. □

Example 2. *For* GQ$(3,1)$*,*

$$N = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

and

$$NN^T = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Two is a relatively low rank for NN^T, making it potentially useful as the parity-check matrix of a quantum code.

Now consider the case where $t = 1$ and s is even. We begin with a lemma that will aid us in computing $\operatorname{rank}_2 NN^T$ for this case.

Lemma 2. *Let M be an $m \times m$ binary matrix, where m is odd. If $M = J - I$, then* $\operatorname{rank}_2 M = m - 1$.

Proof. Each vector in the null space of M (denoted $\text{Null}(M)$) corresponds to a linear combination of the columns of M that yields $\vec{0}$. Note that for binary vectors, a linear combination is identical to a sum of vectors. Every row of M has an even number of ones because m is odd and each row has one zero. Therefore, the sum of all the columns of M is $\vec{0}$, which means that $[1, 1, \ldots, 1] \in \text{Null}(M)$.

Each column of M has a zero in a position in which every other column has a one. Thus the sum of any even number of columns of M will have a one in each position where one of the columns being summed has a zero. Therefore, any vector with an even number of ones is not in $\text{Null}(M)$.

If we choose any odd number of vectors less than m, there will be at least one position in which none of the columns have a zero. Therefore, the sum of these vectors will have a one at that position, so the sum will not be $\vec{0}$. This means that any vector with an odd number of ones and fewer than m ones is not in $\text{Null}(M)$.

Hence, $\text{Null}(M) = \{\vec{0}, [1, 1, \ldots, 1]\}$, and $\dim(\text{Null}(M)) = 1$. Therefore, by Rank-Nullity Theorem, $\operatorname{rank}_2(M) = m - 1$. □

This lemma allows us to determine $\text{rank}_2(NN^T)$ for the case where s is even.

Theorem 2. *Let N be the line-by-point incidence matrix of* $\text{GQ}(s,1)$*. If s is even, then* $\text{rank}_2(NN^T) = 2s+1$*.*

Proof. The structure of NN^T in this case is identical to its structure in the case where s is odd, except that the diagonal of NN^T contains all ones when s is even because each line of $\text{GQ}(s,1)$ is incident with an odd number of points. NN^T is $(2s+2)\times(2s+2)$, and it can be written as four $(s+1)\times(s+1)$ blocks:

$$NN^T = \left[\begin{array}{c|c} I & J \\ \hline J & I \end{array}\right],$$

where I is the $(s+1)\times(s+1)$ identity matrix and J is the $(s+1)\times(s+1)$ matrix of all ones.

The sum of the first $s+1$ rows of NN^T is $\vec{1}$. Thus we can row-reduce NN^T by adding $\vec{1}$ to each of the last $s+1$ rows. This produces the matrix

$$\left[\begin{array}{c|c} I & J \\ \hline 0 & J-I \end{array}\right].$$

The first $s+1$ rows of NN^T are linearly independent of each other because each contains a one in a column where the others contain only zeroes. By the same reasoning, the first $s+1$ rows are also linearly independent of the last $s+1$ rows.

By Lemma 2, $J-I$ has s linearly independent rows, which means that s of the last $s+1$ rows of NN^T are linearly independent. Therefore, NN^T has $2s+1$ linearly independent rows, but all $2s+2$ rows are linearly dependent, so $\text{rank}_2(NN^T) = 2s+1$. □

Since NN^T has $2s+2$ rows and columns, it is nearly full rank in this case, making it less useful for quantum codes than in the case where s is odd.

The observation that $\text{GQ}(s,1)$ can be drawn as a grid allows us to write N in the following way. Note that N is $2(s+1)\times(s+1)^2$. Let the first $s+1$ rows of N represent the lines in one parallel class, and let the other $s+1$ rows represent the lines in the other parallel class. Divide the columns into $s+1$ blocks of $s+1$ columns, and let the first block represent the points incident with the first line, the second block represent the points incident with the second line,..., and the $(s+1)$st block represent the points incident with the $(s+1)$st line. Thus,

$$N = \left[\begin{array}{c|c|c|c|c} 1\ldots1 & 0\ldots0 & 0\ldots0 & \ldots & 0\ldots0 \\ 0\ldots0 & 1\ldots1 & 0\ldots0 & \ldots & 0\ldots0 \\ 0\ldots0 & 0\ldots0 & 1\ldots1 & \ldots & 0\ldots0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0\ldots0 & 0\ldots0 & 0\ldots0 & \ldots & 1\ldots1 \\ \hline I & I & I & \ldots & I \end{array}\right].$$

Theorem 3. *Let N be the line-by-point incidence matrix of* $\mathrm{GQ}(s,1)$. *Then* $\mathrm{rank}_2(N) = 2s+1$.

Proof. The first row of the bottom block of N is the sum of all the other rows of N, so it can be eliminated. In the resulting matrix, every nonzero row has a leading one in a different column. Therefore, the remaining $2s+1$ nonzero rows are linearly independent, so $\mathrm{rank}_2(N) = 2s+1$. □

3.2 $\mathrm{GQ}(1,t)$

Now we consider generalized quadrangles with $s = 1$. $\mathrm{GQ}(1,t)$ is a complete bipartite graph with two sets of $t+1$ vertices. Let $a_1, a_2, \ldots, a_{t+1}$ denote the points in set A, and let $b_1, b_2, \ldots, b_{t+1}$ denote the points in set B. Every line in the generalized quadrangle is incident with one point in each set, and every point is incident with $t+1$ lines.

Each row and each column of NN^T represents a line of the generalized quadrangle. We will arrange the rows of NN^T in $t+1$ blocks of $t+1$ rows such that the jth row in the ith block represents the line that connects a_i to b_j. We will arrange the columns the same way, making the matrix symmetric.

Any two distinct lines through a_i have exactly one point in common. Each line has two points in common with itself. Therefore, by Lemma 1, NN^T has zeroes for its diagonal entries (the entries for which the row and column represent the same line), and ones for the entries where the row and column are in the same block (the entries for which the row and column represent lines through the same point in A). This produces blocks with the form $J-I$ of size $(t+1)\times(t+1)$ down the diagonal of NN^T. For entries outside of these blocks, the row and column represent lines through different points in A. By Lemma 1, these entries are 1 when the row and column represent lines through the same point in B, and 0 otherwise. This produces blocks with the form I of size $(t+1)\times(t+1)$. Therefore,

$$NN^T = \left[\begin{array}{c|c|c|c|c} J-I & I & I & \ldots & I \\ \hline I & J-I & I & \ldots & I \\ \hline I & I & J-I & \ldots & I \\ \hline \vdots & \vdots & \vdots & \ddots & \vdots \\ \hline I & I & I & \ldots & J-I \end{array}\right]$$

Theorem 4. *Let N be the line-by-point incidence matrix of* $\mathrm{GQ}(1,t)$. *Then* $\mathrm{rank}_2(NN^T) = 2t$.

Proof. First, add each row in each block of NN^T to the corresponding row in the block above it to produce the matrix

$$M = \left[\begin{array}{c|c|c|c|c|c|c} J & J & 0 & 0 & \dots & 0 & 0 \\ \hline 0 & J & J & 0 & \dots & 0 & 0 \\ \hline 0 & 0 & J & J & \dots & 0 & 0 \\ \hline 0 & 0 & 0 & J & \dots & 0 & 0 \\ \hline \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \hline 0 & 0 & 0 & 0 & \dots & J & J \\ \hline I & I & I & I & \dots & I & J-I \end{array}\right].$$

Through further row reduction, we can eliminate all but one row in each of the top t blocks to yield

$$\left[\begin{array}{c|c|c|c|c|c|c} 1\dots1 & 1\dots1 & 0\dots0 & 0\dots0 & \dots & 0\dots0 & 0\dots0 \\ 0\dots0 & 1\dots1 & 1\dots1 & 0\dots0 & \dots & 0\dots0 & 0\dots0 \\ 0\dots0 & 0\dots0 & 1\dots1 & 1\dots1 & \dots & 0\dots0 & 0\dots0 \\ 0\dots0 & 0\dots0 & 0\dots0 & 1\dots1 & \dots & 0\dots0 & 0\dots0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0\dots0 & 0\dots0 & 0\dots0 & 0\dots0 & \dots & 1\dots1 & 1\dots1 \\ \hline 0\dots0 & 0\dots0 & 0\dots0 & 0\dots0 & \dots & 0\dots0 & 0\dots0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0\dots0 & 0\dots0 & 0\dots0 & 0\dots0 & \dots & 0\dots0 & 0\dots0 \\ \hline I & I & I & I & \dots & I & J-I \end{array}\right].$$

Clearly, the top t rows are linearly independent, and the bottom $t+1$ rows are linearly independent.

Consider the case where t is odd. Then $t+1$ is even, so the sum of the rows in the last block of M consists of all ones. This is the same as the sum of one row of each of the first, third, fifth, ..., and tth blocks of rows. Thus we can eliminate the top row of the bottom block.

Consider the case where t is even. Then $t+1$ is odd, so the sum of the rows in the last block of M consists of $(t+1)^2-(t+1)$ ones followed by $t+1$ zeroes. This is the same as the sum of one row of each of the first, third, fifth, ..., and $(t-1)$th blocks of rows. Again, we can eliminate the top row of the bottom block.

After eliminating this row, the remaining rows can be rearranged to produce a matrix in echelon form: the top row and the remaining t rows of the bottom block have a pivot in each of the first $t+1$ columns, and the remaining $t-1$ top rows each have a pivot in a different column to the right. Therefore, all of the remaining $2t$ nonzero rows are linearly independent, so $\operatorname{rank}_2(NN^T) = 2t$. □

The lines of $\mathrm{GQ}(1,t)$ are isomorphic to the points of $\mathrm{GQ}(t,1)$ because $\mathrm{GQ}(1,t)$ has $(t+1)^2$ lines, each of which is incident with 2 points, while $\mathrm{GQ}(t,1)$ has $(t+1)^2$ points, each of which are incident with 2 lines. Similarly, the points of $\mathrm{GQ}(1,t)$ are isomorphic to the lines of $\mathrm{GQ}(t,1)$ because $\mathrm{GQ}(1,t)$ has $2(t+1)$ points, each incident with $(t+1)$ lines, while

$\mathrm{GQ}(t,1)$ has $2(t+1)$ lines, each incident with $(t+1)$ points. Therefore, the incidence matrix N of $\mathrm{GQ}(1,t)$ is the transpose of the incidence matrix of $\mathrm{GQ}(t,1)$:

$$N = \left[\begin{array}{cccc|c} 1 & 0 & \dots & 0 & \\ 1 & 0 & \dots & 0 & \\ 1 & 0 & \dots & 0 & I \\ \vdots & \vdots & \ddots & \vdots & \\ 1 & 0 & \dots & 0 & \\ \hline 0 & 1 & \dots & 0 & \\ 0 & 1 & \dots & 0 & \\ 0 & 1 & \dots & 0 & I \\ \vdots & \vdots & \ddots & \vdots & \\ 0 & 1 & \dots & 0 & \\ \hline \vdots & \vdots & \vdots & \vdots & \vdots \\ \hline 0 & 0 & \dots & 1 & \\ 0 & 0 & \dots & 1 & \\ 0 & 0 & \dots & 1 & I \\ \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & \dots & 1 & \end{array}\right].$$

Theorem 5. *Let N be the line-by-point incidence matrix of* $\mathrm{GQ}(1,t)$. *Then* $\mathrm{rank}_2(N) = 2t+1$.

Proof. Add the first row in each block of N to each other row within the block to produce

$$\left[\begin{array}{cccc|cccc} 1 & 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 1 & 1 & \dots & 0 \\ 0 & 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 1 & 0 & \dots & 1 \\ \hline 0 & 1 & \dots & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 1 & 1 & \dots & 0 \\ 0 & 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 1 & 0 & \dots & 1 \\ \hline \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \hline 0 & 0 & \dots & 1 & 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 1 & 1 & \dots & 0 \\ 0 & 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 1 & 0 & \dots & 1 \end{array}\right].$$

The second through $(t+1)$th rows of the second through $(t+1)$th blocks are redundant and can be eliminated because they are identical to the second through $(t+1)$th rows of the first block. The remaining rows are then linearly independent because each contains a one in a column where every other row has a zero. There are $t+1$ of these rows in the first block and one in each of the other t blocks, so $\text{rank}_2(N) = 2t+1$.

□

4 Quantum Codes

We will now construct some examples of EAQECCs from generalized quadrangles. Recall that the parameters of a quantum code with $m \times n$ parity-check matrix N are $[[n, n - 2\,\text{rank}_2(N) + \text{rank}_2(NN^T); \text{rank}_2(NN^T)]]$ [1, 2].

Theorem 6. *If N is the line-by-point incidence matrix of $\text{GQ}(s,1)$ and s is odd, then there exists a quantum code with parameters $[[(s+1)^2, s^2-2s+1; 2]]$.*

Proof. By Theorems 1 and 3, $\text{rank}_2(NN^T) = 2$ and $\text{rank}_2(N) = 2s+1$. N is $2(s+1)\times(s+1)^2$. Thus, by Proposition 1, there exists a quantum code with parameters $[[(s+1)^2, s^2-2s+1; 2]]$. □

This code uses a conveniently small number of ebits.

Theorem 7. *If N is the line-by-point incidence matrix of $\text{GQ}(s,1)$ and s is even, then there exists a quantum code with parameters $[[(s+1)^2, s^2; 2s+1]]$.*

Proof. By Theorem 2, $\text{rank}_2(NN^T) = 2s+1$. As in the previous theorem, $\text{rank}_2(N) = 2s+1$ and N is $2(s+1)\times(s+1)^2$. Therefore, by Proposition 1, there exists a quantum code with parameters $[[(s+1)^2, s^2; 2s+1]]$. □

As noted above, NN^T is nearly full rank in this case, which means that the code uses a relatively large number of ebits.

Theorem 8. *If N is the line-by-point incidence matrix of $\text{GQ}(1,t)$, then there exists a quantum code with parameters $[[2t+2, 0; 2t]]$.*

Proof. By Theorems 4 and 5, $\text{rank}_2(NN^T) = 2t$ and $\text{rank}_2(N) = 2t+1$. Therefore, by Proposition 1, there exists a quantum code with parameters $[[2t+2, 0; 2t]]$. □

This code has $k = 0$, which means that the code exists in a linear space of dimension 0 and is therefore not useful.

5 Conclusion

We have determined $\text{rank}_2(NN^T)$ for $\text{GQ}(1,t)$ and $\text{GQ}(s,1)$, and we have used these results to compute the parameters of quantum codes defined by the incidence matrices of these generalized quadrangles. The following open questions about other classes of generalized quadrangles provide a good starting point for future research on this topic.

Question 1. *What is* $\text{rank}_2(NN^T)$ *for* $\text{GQ}(2,t)$*?*

Question 2. *What is* $\text{rank}_2(NN^T)$ *for* $\text{GQ}(s,2)$*?*

Questions 1 and 2 are the next level up in complexity from our results. Ultimately, we would like to be able to create quantum codes from any generalized quadrangle. This problem is stated in Question 3.

Question 3. *What is* $\text{rank}_2(NN^T)$ *for* $\text{GQ}(s,t)$ *in general?*

In addition, further research could focus on other substructures in finite geometries that might also be sources of good quantum error-correcting codes.

References

[1] Y. Fujiwara, D. Clark, P. Vandendriessche, M. De Boeck, V. D. Tonchev, *Entanglement-assisted quantum low-density parity-check codes*, Physical Review A **82** (2010), 1–19.

[2] T. Brun, I. Devetak, M. H. Hsieh, *Correcting quantum errors with entanglement*, Science 314 (2006), 436–439.

[3] S. E. Payne, J. A. Thas, *Finite Generalized Quadrangles, Second Edition*, European Mathematical Society (2009).