ISIT2001, Washington, DC, June 24–29, 2001

Construction of Codes Based on Finite Generalized Quadrangles for Iterative Decoding

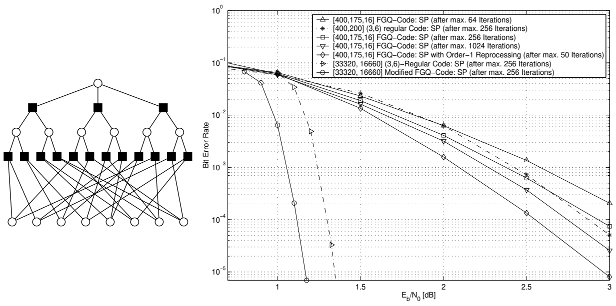
Pascal O. Vontobel[1]
ISI, EE Deptartment, ETH Zurich
Sternwartstr. 7, CH-8092 Zurich
e-mail: vontobel@isi.ee.ethz.ch

R. Michael Tanner
CS Department, UC Santa Cruz
Santa Cruz, CA 95064, USA
e-mail: tanner@cse.ucsc.edu

Abstract — **Finite generalized polygons (FGPs) for constructing Tanner graphs are investigated, focusing on finite generalized quadrangles (FGQs). Graphs from FGPs are distinctive in that their girths are the largest possible, namely, exactly twice the diameter. Rates, minimum distances, and simulation results using enhanced sum-product decoders are given.**

I. Introduction

Using finite geometries and incidence structures to construct codes is well-known (see, e.g. [1]). Our goal is to construct Tanner graphs that have large girth, in order to assure greatest independence of the messages when the associated codes are iteratively decoded. Some of the codes that we will derive from FGPs are also special in that they result in highly redundant parity-check matrices, i.e. a large fraction of the rows of the parity-check matrix are linearly dependent. Codes based on finite projective planes have the same property and they have recently been recognized to have good decoding performance (see, e.g. [2]). Indeed, these codes have graphs that are derived from generalized triangles, a special case.



II. Point-Line Incidence Structures and Finite Generalized Polygons

Let $\mathcal{S} = (\mathcal{P}, \mathcal{L}, \mathtt{I})$ be an incidence structure with the point set $\mathcal{P}$, the line set $\mathcal{L}$, and the incidence relation $\mathtt{I} \subseteq \mathcal{P} \times \mathcal{L}$. We say that a point $p \in \mathcal{P}$ is incident on (or lies on) a line $L \in \mathcal{L}$ if and only if $(p, L) \in \mathtt{I}$. To an incidence structure $\mathcal{S}$ we can associate a (bipartite) graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ with the vertex set $\mathcal{V} = \mathcal{P} \cup \mathcal{L}$, and there is an edge connecting two vertices if and only if there is an incidence relation between these two vertices. FGPs, introduced by Tits [3], are point-line incidence structures where all points are on exactly $t+1$ lines, all lines have exactly $s+1$ points and whose associated graph has the property that the girth is exactly twice the diameter, which is the largest possible. A generalized n-gon therefore has by definition diameter n and girth $2n$; (s,t) is called the order of the FGP. Of course, an *ordinary* polygon is an FGP of order $(1,1)$. By a result of Feit and Higman, interesting (t>1 and s>1) FGPs are known to exist only for $n = 2, 3, 4, 6, 8$. An FGQ with parameters $(s,t) = (2,2)$ is shown on the left hand side of the figure. For FGQs, a simple counting argument gives $|\mathcal{P}| = (s+1)(st+1)$ and $|\mathcal{L}| = (t+1)(st+1)$.

[1]This work was done while visiting UC Santa Cruz. Supported by Grant TH-16./99-3.

III. Construction of Codes

Special cases of codes derived from FGQs have been considered by Bagchi, Sastry, Brouwer and others some ten years ago (see, e.g. [4]). We consider two possible classes of codes. In class $\mathsf{C}^{(1)}$ we define the point vertices to be bit nodes and the line vertices to be check nodes (simple parity-checks or more complicated constraints). If the FGQ has order (s,t) then each bit node is connected to $t+1$ check nodes and each check node to $s+1$ bit nodes and the code has length $(s+1)(st+1)$. Lower bounds on the minimum distance (which here are often tight) can be derived analytically by using the so-called "bit-" and "parity-oriented bounds" of [5]. A second class $\mathsf{C}^{(2)}$ can be defined in the following way: point and line vertices are check nodes and on each edge we add a new bit node of degree two. To define strong codes, more restrictive (and more computationally expensive) subcode constraints must be imposed at the points and lines of the FGQ. The right hand side of the figure shows the bit error rate for a $[400, 175, 16]$ code of class $\mathsf{C}^{(1)}$ derived from an FGQ with $(s,t) = (7,7)$ under sum-product decoding and sum-product decoding with Fossorier's first-order reprocessing compared with a random $(3,6)$-regular length-400 rate-1/2 code. We also show the bit error rate of a length-33320 rate-1/2 code from class $\mathsf{C}^{(2)}$ based on an FGQ with $(s,t) = (13,13)$ with $[14,10,3]$ and $[14,11,2]$ constraint codes compared with a random $(3,6)$-regular rate-1/2 code of the same length ([6] presents a comparable code with similar performance gains.). For encoding of these codes, especially from the first class, one can use their group properties as each FGQ is tightly connected to a specific group.

References

[1] S. Lin and D. J. Costello, Jr., *Error Control Coding: Fundamentals and Applications.* Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1983.

[2] R. Lucas, M. Fossorier, Y. Kou, and S. Lin, "Iterative Decoding of One-Step Majority Logic Decodable Codes Based on Belief Propagation," vol. COMM-48, pp. 931–937, June 2000.

[3] J. Tits, "Sur la Trialité et Certains Groupes qui s'en Déduisent," *Inst. Hautes Etudes Sci. Publ. Math.*, vol. 2, pp. 14–60, 1959.

[4] B. Bagchi and N. S. N. Sastry, "Even Order Inversive Planes, Generalized Quadrangles and Codes," *Geom. Dedicata*, vol. 22, no. 2, pp. 137–147, 1987.

[5] R. M. Tanner, "Minimum Distance Bounds by Graph Analysis," *accepted for publication in IEEE Trans. Inform. Theory.*

[6] J. Lafferty and D. Rockmore, "Codes and Iterative Decoding on Algebraic Expander Graphs," in *Proc. of Intern. Symp. on Inform. Theory and its Appl.*, (Hawaii, USA), 2000.