Improved constructions of quantum codes from the Hermitian curve

René Bødker Christensen

Aalborg University

rene@math.aau.dk

Abstract. Ruud Pellikaan and coauthors in *Handbook of Coding Theory* introduced the order bound for a family of codes described in terms of their parity check matrices. This bound furthermore implies a method for improving the parameters. The bound was later enhanced to also work for primary codes. In this work, we employ the above methods to construct improved quantum codes from the Hermitian curve.

The CSS construction translates a pair of nested linear codes $C_2 \subsetneq C_1 \subseteq \mathbb{F}_q^n$ into a quantum code with parameters $[[n, k, d_z/d_x]]_q$ where d_z is the minimum distance related to phase-shift errors and d_x is the minimum distance related to bit-flip errors. Here, $k = \dim C_1 - \dim C_2$ is the codimension of C_1 and C_2, and $d_z = d(C_1, C_2)$ and $d_x = d(C_1^\perp, C_2^\perp)$ are given by the relative distances of the codes and their duals. When $d_z \neq d_x$, we speak of asymmetric quantum codes. In some situations, however, we are not interested in distinguishing between the two types of errors. In this case, we let $d = \min\{d_z, d_x\}$, and write the corresponding code parameters as $[[n, k, d]]_q$. Given appropriate codes $C_2 = C_1^\perp \subsetneq C_1 \subsetneq C_0$, the Steane enlargement method produces an $[[n, k, \geq d]]_q$ quantum code where $k = 2\dim C_1 - n + (\dim C_0 - \dim C_1)$ and $d = \min\{d(C_1), (1 + \frac{1}{q})d(C_0)\}$.

In this work, we apply the CSS construction and Steane's enlargement to codes constructed from the Hermitian curve. For the CSS construction we consider two cases. Namely, Case 1 where C_1 is an order bound improved code, and C_2 is the dual of an order bound improved code; and Case 2 where both C_1 and C_2 are ordinary one-point algebraic geometric codes, but at least one of the relative distances exceeds the corresponding non-relative one. In Case 3 we apply Steane's enlargement to order bound improved codes C_1 and C_0 (where of course $C_1^\perp \subsetneq C_1$). Doing this, we obtain very good quantum codes. Closed formula expressions for and estimates on the parameters of the codes are provided along with tables demonstrating the advantage of the construction. Here, we list only a few samples of code parameters.

Case 1	**Case 2**	**Case 3**
$[[27, 2, 23/2]]_9$	$[[27, 1, 20/4]]_9$	$[[27, 11, 7]]_9$
$[[27, 6, 12/6]]_9$	$[[64, 1, 46/9]]_{16}$	$[[64, 60, 3]]_{16}$
$[[27, 11, 11/3]]_9$	$[[64, 4, 49/4]]_{16}$	$[[64, 36, 10]]_{16}$
$[[64, 18, 36/4]]_{16}$	$[[125, 2, 86/20]]_{25}$	$[[125, 91, 11]]_{25}$
$[[125, 80, 28/5]]_{25}$	$[[125, 3, 91/15]]_{25}$	$[[125, 117, 4]]_{25}$

Table 1: Sample parameters for quantum codes in each of the cases 1, 2, and 3.

Joint work with Olav Geil (Aalborg University)