dual code

Canonical name	DualCode
Date of creation	2013-03-22 15:13:29
Last modified on	2013-03-22 15:13:29
Owner	GrafZahl (9234)
Last modified by	GrafZahl (9234)
Numerical id	6
Author	GrafZahl (9234)
Entry type	Definition
Classification	msc 94B05
Related topic	LinearCode
Related topic	OrthogonalComplement
Defines	self-dual
Defines	self-orthogonal

Let C be a linear code of block length n over the finite field $\mathbb{F}_q$. Then the set

$$C^{\perp} := \{d \in \mathbb{F}_q^n \mid c \cdot d = 0 \text{ for all } c \in C\}$$

is the *dual code* of C. Here, $c \cdot d$ denotes either the standard dot product or the Hermitian dot product.

This definition is reminiscent of orthogonal complements of http://planetmath.org/node/539 dimensional vector spaces over the real or complex numbers. Indeed, $C^{\perp}$ is also a linear code and it is true that if k is the http://planetmath.org/node/5398dimension of C, then the of $C^{\perp}$ is $n-k$. It is, however, **not** necessarily true that $C \cap C^{\perp} = \{0\}$. For example, if C is the binary code of block length 2 http://planetmath.org/node/806spanned by the codeword $(1,1)$ then $(1,1)\cdot(1,1) = 0$, that is, $(1,1) \in C^{\perp}$. In fact, C equals $C^{\perp}$ in this case. In general, if $C = C^{\perp}$, C is called *self-dual*. Furthermore C is called *self-orthogonal* if $C \subseteq C^{\perp}$.

Famous examples of self-dual codes are the extended binary Hamming code of block length 8 and the extended binary Golay code of block length 24.