



THE CHINESE UNIVERSITY OF HONG KONG  
 Institute of Network Coding  
 and  
 Department of Information Engineering  
*Seminar*



## Code Constructions and Existence Bounds for the Relative Generalized Hamming Weight

by

**Prof. Yuan LUO (駱源教授)**  
**Shanghai Jiao Tong University, China**

**Date** : ~~2 August 2012 (Thursday)~~ **8 August 2012 (Wednesday)**  
**Time** : 2:30 - 3:30 pm  
**Venue** : **Room 833, Ho Sin Hang Engineering Building**  
**The Chinese University of Hong Kong**

### Abstract

The relative generalized Hamming weight (RGHW) of a linear code  $C$  and a subcode  $C_1$  is an extension of generalized Hamming weight (GHW). The concept was firstly used to protect messages from an adversary in the wiretap channel of type II with illegitimate parties. It was also applied to the wiretap network II for secrecy control of network coding and to trellis-based decoding algorithms for complexity estimation.

For RGHW, bounds and code constructions are two related issues. Upper bounds on RGHW show the possible optimality for the applications, and code constructions meeting upper bounds are for designing optimal schemes. Here, we show indirect and direct code constructions for known upper bounds on RGHW. When upper bounds are not tight or constructions are hard to find, we provide two asymptotically equivalent existence bounds about good code pairs for designing suboptimal schemes. Particularly, most code pairs  $(C, C_1)$  are good when the length  $n$  of  $C$  is sufficiently large, the dimension  $k$  of  $C$  is proportional to  $n$  and other parameters are fixed. Moreover, the first existence bound yields an implicit lower bound on RGHW, and the asymptotical form of this existence bound generalizes the usual asymptotical Gilbert-Varshamov bound.

### Biography

Dr. Luo received the B.S. in (Mathematics) Information Science, M.S. and Ph.D. degrees in Probability and Mathematical Statistics from Nankai University, China, in 1993, 1996, and 1999, respectively. From July 1999 to April 2001, he held a Postdoctoral position in the Institute of Systems Science, Chinese Academy of Sciences. From May 2001 to April 2003, he had a Postdoctoral position in the Institute for Experimental Mathematics, University of Duisburg-Essen, Germany. Since June 2003, he has been with the Computer Science and Engineering Department, Shanghai Jiao Tong University, Shanghai, China. He held his present position as a Full Professor since 2006. His research interests include Information Theory (especially Shannon Channel Capacity), Coding Theory (especially Hamming Distance, Constant Composition and Constant Weight Code, Periodic Sequence) and Computer Security (especially Virtual Machine Security).

**\*\*ALL ARE WELCOME \*\***