

0368-3072 – Error Correcting Codes

Sundays, 14:00-17:00 in Shenkar (physics) 104.

Grading policy:

- Exam – 50%.
- Homework – 50%.
- Bonuses for help in forum and active participation in class.

References Abbreviation Table

[R]	Ron M. Roth	Introduction to Coding Theory (library link)
[HP]	W. Cary Huffman and Vera Pless	Fundamentals of Error Correcting Codes (library link)
[GRS]	Venkatesan Guruswami, Atri Rudra and Madhu Sudan	Essential Coding Theory (link)
[S]	Madhu Sudan	Essential Coding Theory lecture notes (link)
[G]	Venkatesan Guruswami	Introduction to Coding Theory lecture notes (link)

Extended Syllabus

Part I – The basic problem and some basic constructions		
Error correction basics	Linear codes. Distance and dimension. Encoding and decoding. The generator matrix. The dual code. The parity-check matrix.	R 2 HP 1.2-1.4
	Hamming codes (distance, dimension, encoding, decoding, perfect).	GRS 2.4 Handout 1
	Hadamard codes (distance, dimension, encoding, decoding).	Handout 1
Basic algebra: Groups and Finite Fields Basic codes Basic AG codes	Polynomials. Irreducible polynomials. Finite fields. Minimal polynomial, Generators.	R 3 GRS 5.1
	Number of roots of a polynomial. The Reed-Solomon (RS) code (distance, dimension, encoding, no decoding yet). The dual of a RS code.	GRS 5.2 Handout 1
	Reed-Muller (RM) codes. The dual of a RM code is a RM code.	S 4 Handout 1
	Cyclic codes. Polynomial codes. RS is cyclic. The dual of a cyclic code is cyclic.	R 8.1-8.2 Handout 2
	The Hamming code is cyclic.	R 8.2 Handout 2
	Number of common roots of two polynomials. Hermitian codes (encoding only). A glimpse towards AG codes.	Handout 1
Concatenation	RS concatenated with Hadamard (encoding only). Nested concatenation.	GRS 9.1 Handout 3
	Hermitian concatenated with Hadamard (encoding only).	Handout 3
	Naive decoding.	GRS 11.1
	Improved decoding: The GMD (generalized minimum distance) decoding algorithm.	GRS 11.3
	The Justensen code (encoding and decoding).	GRS 9.3
Part II – Decoding RS and List decoding		

Non-unique decoding	Stochastic noise.	GRS 6
	List decoding.	GRS 7.2
	The Johnson's bound.	GRS 7.3 G 4
Explicit List decoding	Welch-Berlekamp's algorithm. Error locating polynomials.	GRS 13.1
	List decoding RS codes.	GRS 13.2
	Parvaresh-Vardy codes.	
	Folded RS codes.	GRS 14

Part III – What is possible and what is not. What is explicit and what is not

Rate vs. Distance Lower Bounds	The Singleton bound.	G 4
	The Hamming bound.	HP 1.12, 2.10.3
	The Plotkin bound.	G 4
	The Elias-Bassalygo bound.	GRS 8.1 G 4
	The Linear Programming (LP) bounds (just stating the result).	HP, 2.10.5
Rate vs. Distance Upper Bounds	The Gilbert-Varshamov (non-explicit) bound.	GRS 4.2 G 2
	RS, Hadamard, Hamming, AG codes.	
Rate vs. List-Decoding distance	Non-explicit and lower bound.	GRS 7.4
	Explicit bounds for: RS, PV, Folded RS, Binary codes.	

Part IV – Codes and Graphs

Expander Codes	Expanders: Graphs that sparsify the complete graph.	
	The Sipser-Spielman LDPC codes.	GRS 10
Good codes with distance close to half	Bias of a distribution (w.r.t. linear tests). The Fourier transform.	
	Error correcting codes and small-bias sets.	
	A code with distance close to half using random walks on expanders (encoding only).	

