格子に基づく符号理論の協調通信・セキュリティへの応用

Lattice Coding Theory for Cooperative Communications and Security

チュートリアルセッション AT-1

電子情報通信学会ソサイエティ大会

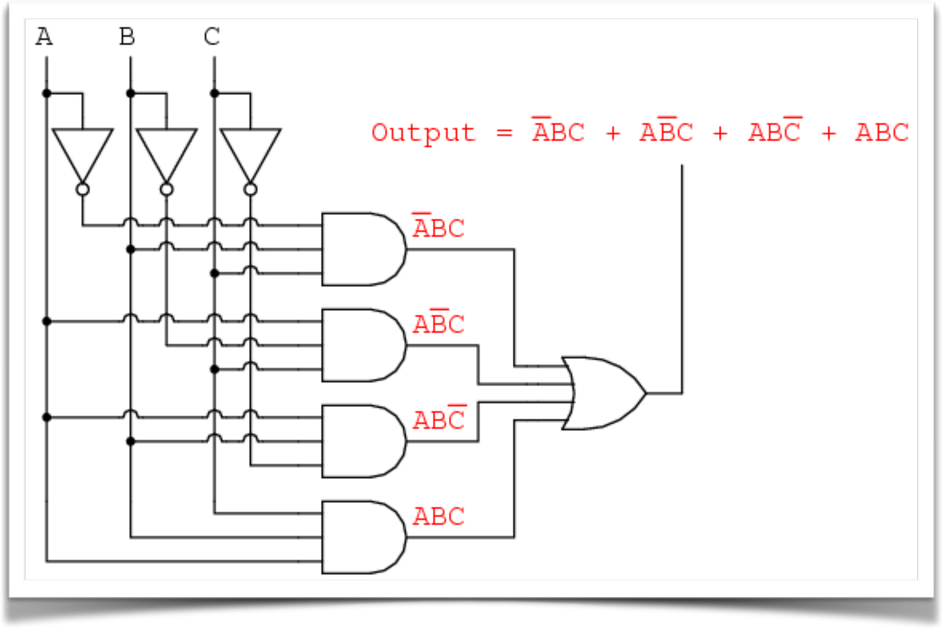
2015年9月11日　9:00〜12:00

Cooperative Wireless Networks

Wireless networks must deal with fading, interference & noise

Error Correcting Codes over Finite Fields

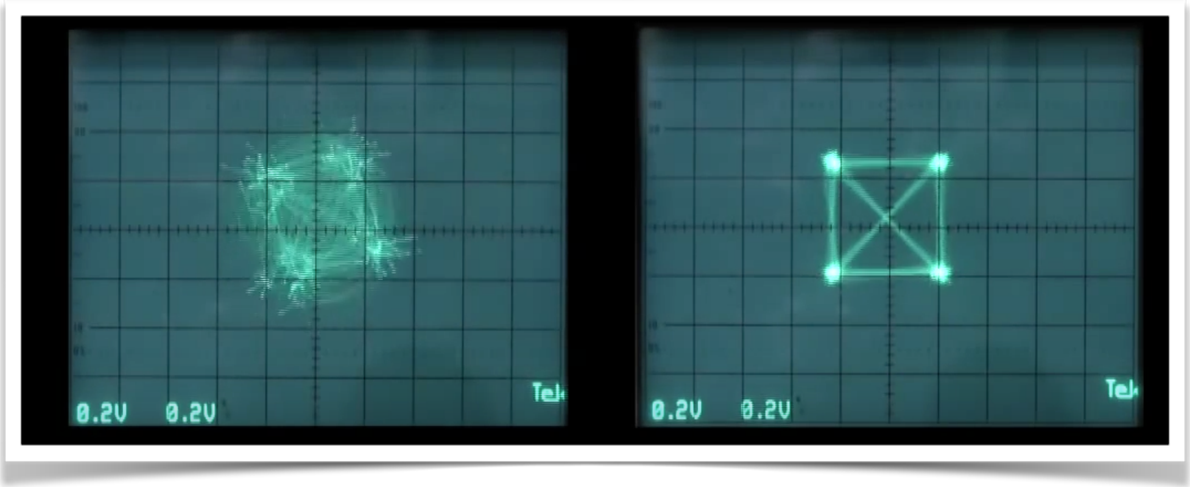
Computers are digital
Finite field codes are highly suited
(and widely used)



A circuit

Error Correcting Codes over Real Numbers

The world is full of real-valued signals
Finite fields are not “signals”
Lattices are codes over real numbers



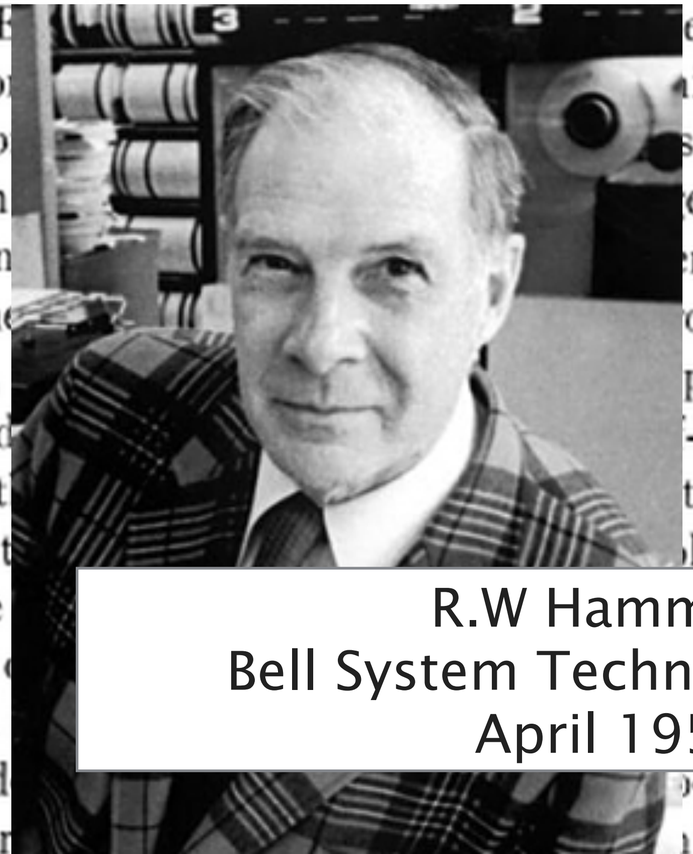
QAM constellation

Error Correcting Codes over Finite Fields

Error Detecting and Error Correcting Codes

By R. W. HAMMING

1. INTRODUCTION



en in this paper from a c
ines in which a large n
single error in the end re
e scale is not essentially
ry large number of opera
ong numbers are kept w
pletely eliminated. This
-checking circuits. The o
till detected by the custo
laint, while if it is transie
e done until the failure
then it invalidates all su

R.W Hamming
Bell System Technical Journal,
April 1950

Lattices are Codes over Real Numbers

26.

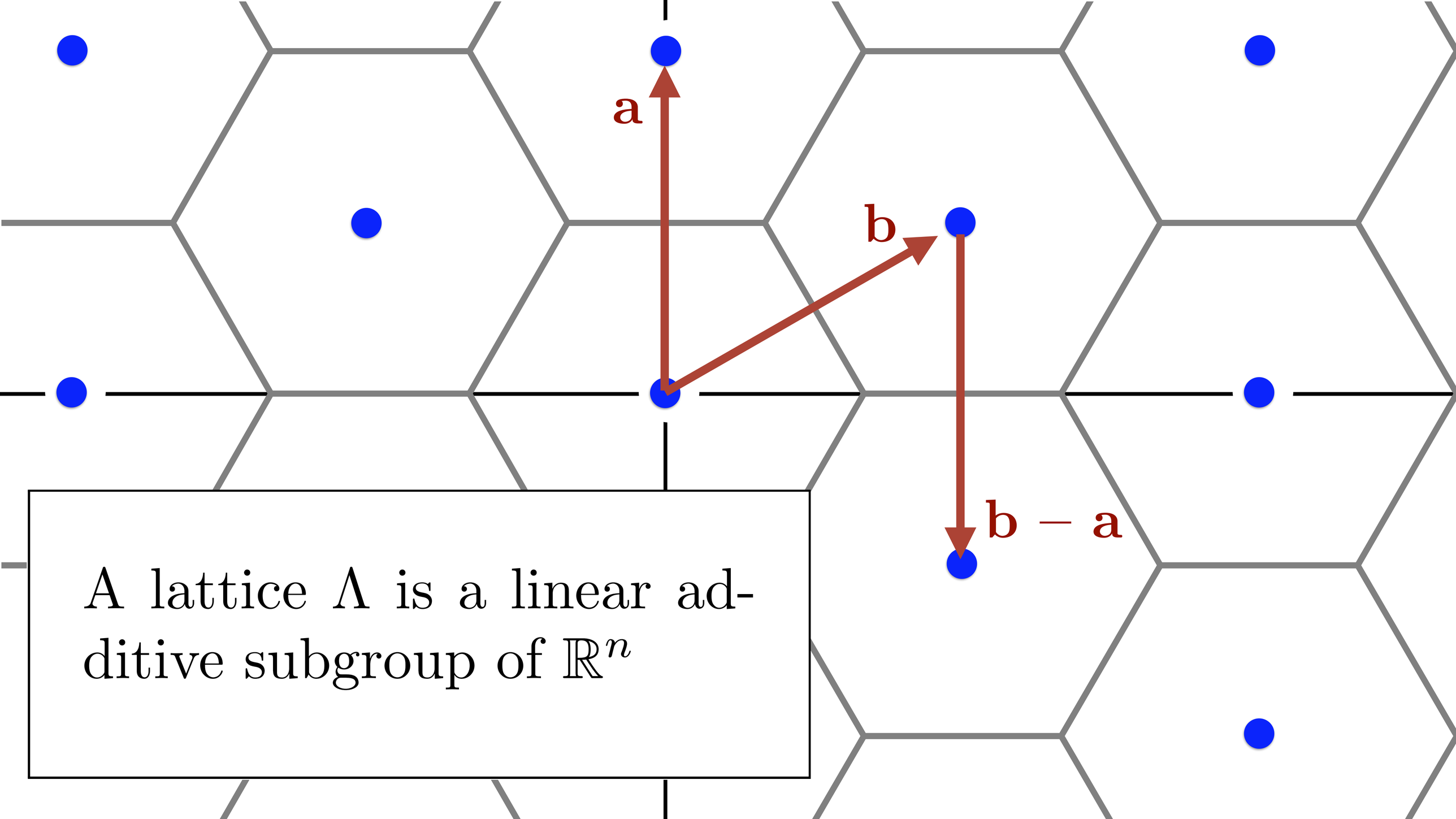
Extraits de lettres de M. Ch. Hermite à M. Jacobi sur différents objets de la théorie des nombres.

(Continuation de ces lettres au cahier précédent.)

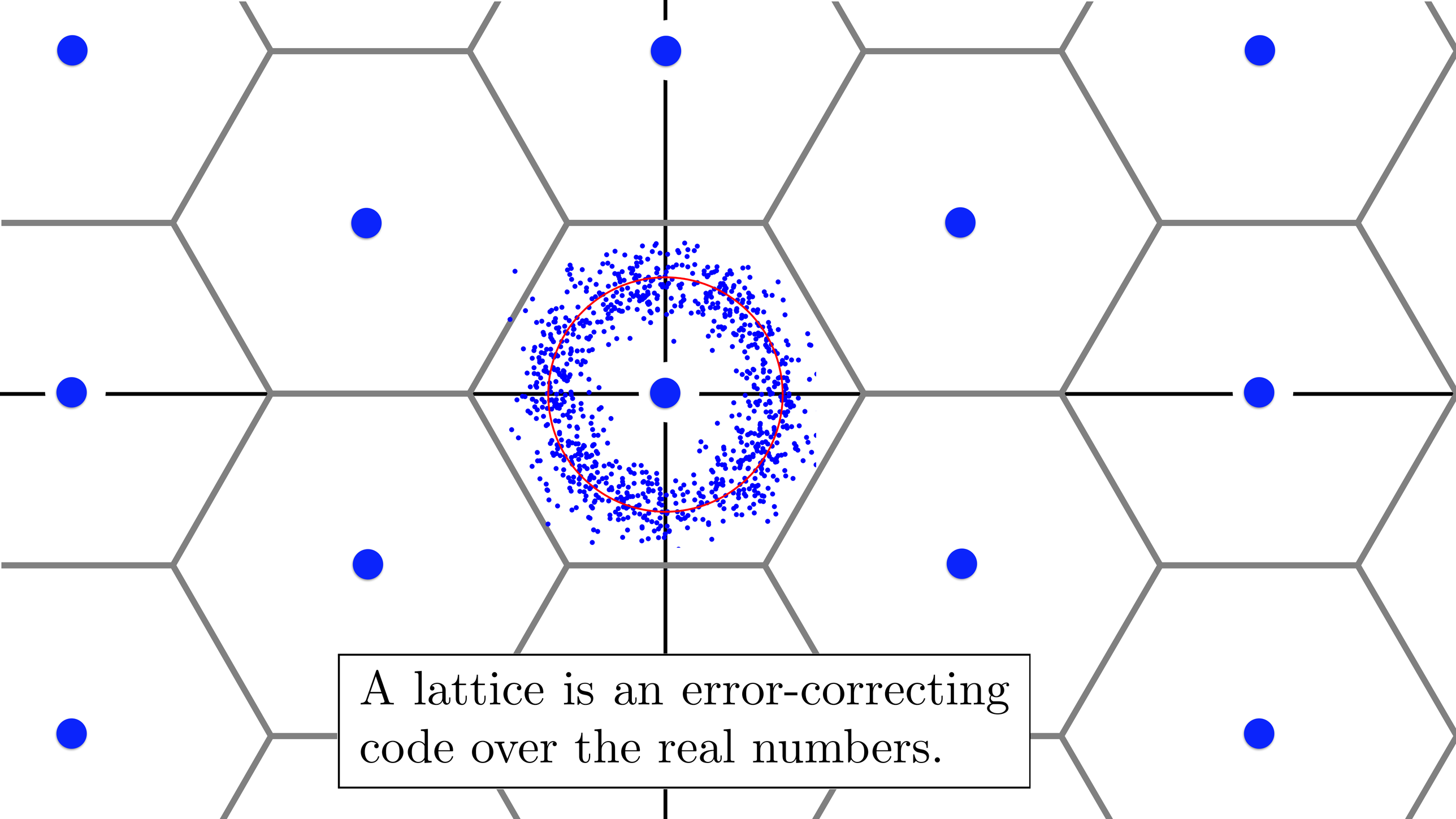
Deuxième lettre.

Permettez-moi de venir enco
de rencontrer sur la théorie des form
que j'ai eu l'honneur de Vous écrire.
ma lettre, la démonstration de cette p
déterminant, de se laisser distribuer e
été amené à une méthode de réducti
à l'algorithme de *Lagrange* pour le
Monsieur, pour me pardonner, s'il m'a
que je n'ai pas encore suffisamment m
immense étendue, je cède au plaisir
placés à l'abord de questions difficiles

C. Hermite
Journal für die reine und angewandte
Mathematik, 1850



A lattice Λ is a linear additive subgroup of $\mathbb{R}^n$



A lattice is an error-correcting code over the real numbers.

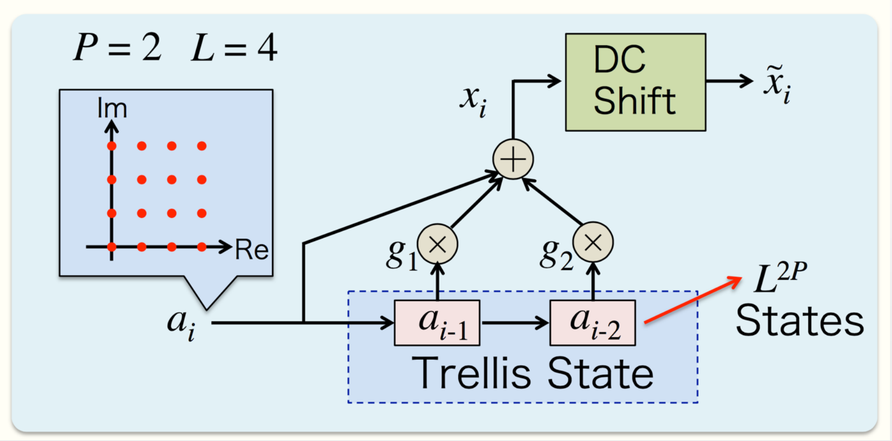
Program

9:10-9:50	格子の畳込み符号への応用：Signal CodesとTurbo Signal Codes	落合秀樹（横浜国大）
9:50-10:30	重畳符号化を用いた協調通信	林　和則（京大）
10 min		
10:40-11:20	格子に基づく暗号・暗号解析入門	國廣　昇（東大）
11:20-12:00	An Introduction to Physical Layer Network Coding: Lattice Codes as Groups	Brian Kurkoski（JAIST）

1 格子の畳込み符号への応用：Signal CodesとTurbo Signal Codes・

落合秀樹（横浜国大）

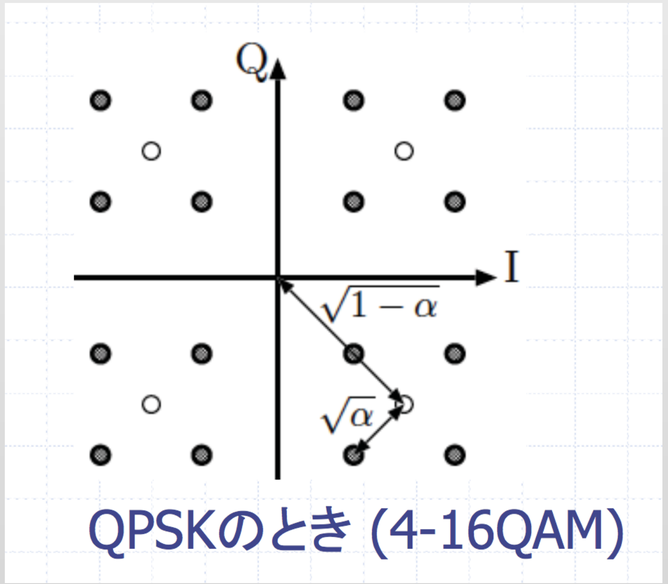
・Recent lattice constructions approach capacity (unconstrained)
・Signal codes are a “convolutional lattice code” which are well-suited for wireless communications



2 重畳符号化を用いた協調通信

林　和則（京大）

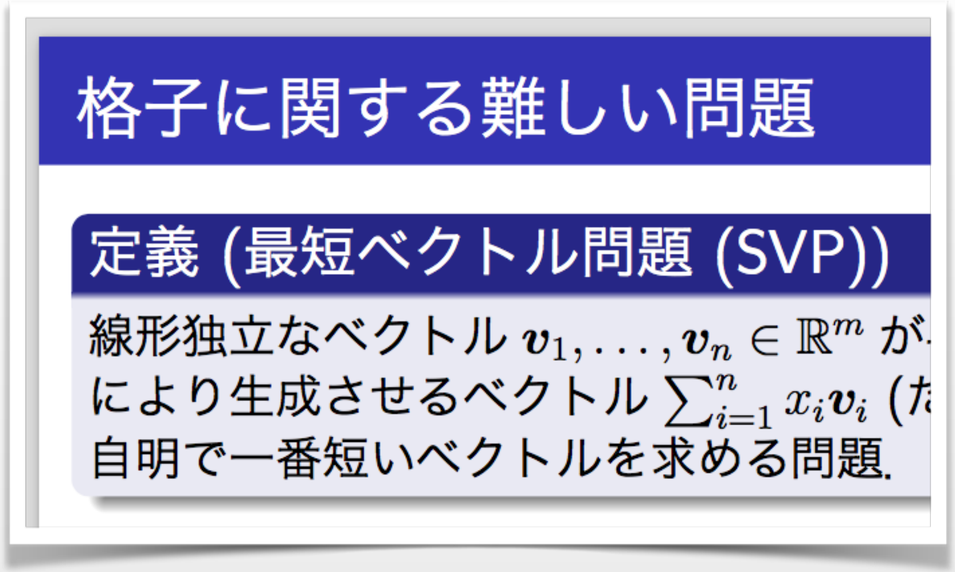
・Superposition coding deals with broadcast phase of relay channel
・Requires careful constellation design
・Cooperative communications tightly connected to lattices.



3 格子に基づく暗号・暗号解析入門・

國廣　昇（東大）

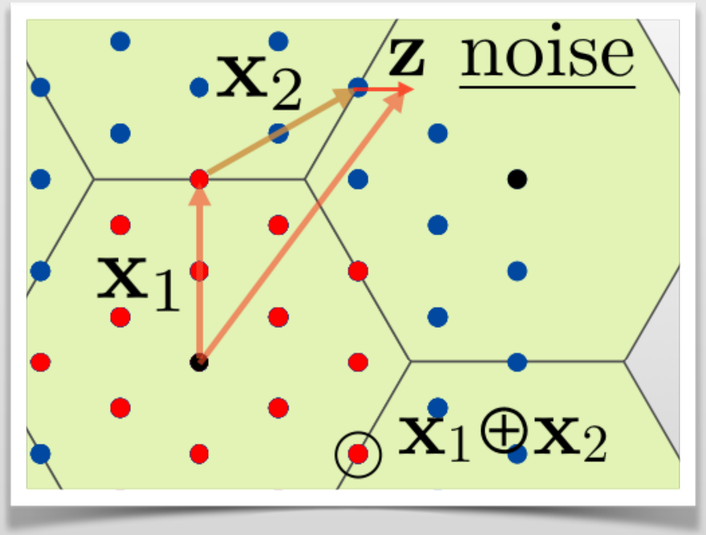
・Cryptography based on lattices
・Computational hardness of finding shortest vector problem
・Not wireless communications!



4 An Introduction to Physical Layer Network Coding

Brian Kurkoski（JAIST）

・Physical layer network coding for wireless networks
・Combat interference and increase throughput
・Tutorial on nested lattice codes



Thank you

Speakers

- Hideki Ochiai
- Kazunori Hayashi
- Noboru Kunihiro

Tutorial Session Co-Organizers

- Hiroshi Kamabe (Gifu University)
- Yasutada Oohama (University of Electro-Communications)

Session Chairs:

- Hideki Ochiai (Yokohama National University)
- Kazushi Mimura (Hiroshima City Univesity)