Partial independence, and secret sharing

Do there exist events E_1, E_2, E_3, E_4 such that

- Any 2 events are independent
- Any 3 events are not IND. ?

YES!

MODULAR ARITHMETIC mod 5

$x \bmod 5 :=$ remainder of x divided by 5.

$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$. we can $+, -, \times, \div$ modulo 5

These numbers wrap around:

$4+2 \bmod 5 = 1$ $\qquad$ $2-4 \bmod 5 = -2 \bmod 5$
$= 3$

$2 \times 4 \bmod 5 = 3.$

$0 \times ? \bmod 5 = 0.$

For division, first exclude "divided by 0".

Then: $1 \div x :=$ number y s.t. $y \cdot x = 1$

Unless $x=0$, y is uniquely determined

$1 \div 1 = 1$

$1 \div 2 = 3$

$1 \div 3 = 2$

$1 \div 4 = 4$

finite field

Construct this:

$\Omega = \{(A, B)$: rolls of 2 5-sided dice$\}$.

Assume equally likelihood outcomes. ($1/25$)

Let $E_1 =$ "$A+B=0$", $E_2 =$ "$2A+B=0$",

$E_i =$ " $iA + B = 0$ ". all arithmetic is mod 5

$P(E_2) = P(2 \cdot A + B = 0)$

A :	1	2	3	4	5
$2A$:	2	4	6	8	10
$2A$ mod 5 :	2	4	1	3	0

unique

$\Rightarrow \forall\ 2A$, we have a unique value of B s.t.
$2A + B = 0 \pmod 5$

$\Rightarrow P(2A+B=0) = \sum_{2A} P(2A+B=0 \mid 2A) \cdot P(2A)$

$= 5 \cdot \left(\frac{1}{5} \cdot \frac{1}{5}\right) = \frac{1}{5}$

$\Rightarrow P(iA + B = 0 \mid A = a) = \frac{1}{5}$, and $P(iA+B) = \frac{1}{5}$

Now,

$P(E_1 \cap E_2) = P\begin{pmatrix} A+B=0 \\ 2A+B=0 \end{pmatrix} \geq \frac{1}{25}$ $\underline{(A=0, B=0)}$ only solution

System of equations: $\Rightarrow \begin{cases} A+B=0 \\ A=0 \end{cases} \Rightarrow$

And, $P(E_2 \cap E_4)$:

$\begin{matrix} 2A+B=0 \\ 4A+B=0 \end{matrix} \Rightarrow \begin{matrix} 2A+B=0 \\ 2A=0 \end{matrix} \Rightarrow \begin{matrix} A=0 \\ B=0. \end{matrix}$

$\Rightarrow P(E_i \cap E_j) = \frac{1}{25} = P(E_i) \cdot P(E_j)$ ✓

Now look at $\forall$ 3 events:

$P(E_1 \cap E_2 \cap E_4) = P\begin{pmatrix} A+B=0 \\ 2A+B=0 \\ 4A+B=0 \end{pmatrix} = \frac{1}{25}$. not IND.

Secret sharing (Application of the above)

Dealer S

Alice	Bob	Charlie
X_1	X_2	X_3

parts of secret.

I construct the partial secret s.t.:

1. None of the people alone know what S is
2. $\forall$ two people can recover S

To achieve this, let $S \in \{0,1,2,3,4\}$,

$X_i = A \cdot i + S$, where A is a random number mod 5

Say Bob & Dave,

Bob $X_2 = 2A + S$

Dave $X_4 = 4A + S$.

again system of equations, can solve for A and S.

$S = 2X_2 - X_4 \mod 5$

Look at say Charlie alone: $X_3 = 3A + S$.

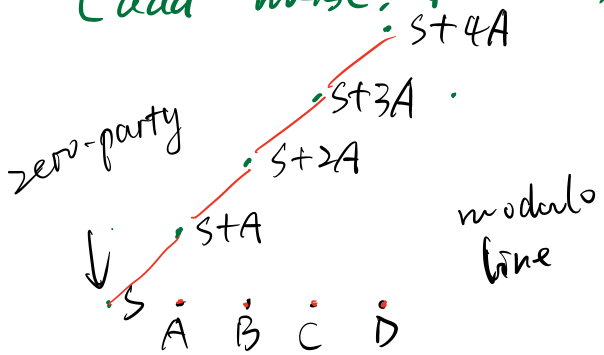
cannot determine S <u>as A is random</u>

For 5 people A B C D: $\forall$ 3 of 4 can recover S,

but not $\forall$ 2 of them.

Obviously, need more unknowns (equations)

(add noise, or "salt", to the information)



$l(t) = At + S$

$S = l(0)$. $X_i = l(i) = Ai + S$

So, let $q(t) = At^2 + Bt + S$.

$S = q(0)$, $X_i = q(i)$

$\forall$ 3 q's, e.g. $q(1)$, $q(3)$, $q(4)$, can solve for A, B, S.

$\forall$ 2 q's, do not have any info for S.

Always possible to do this for $\forall$ $1 \le t \le n$,

- n parties in total
- $\forall$ t can recover the secret
- $\forall$ $t-1$ or fewer cannot, i.e. they see equally likely outcomes.