Regarding the article

Paradigm – 20 Jul 21

Ethereum Reorgs After The Merge

There has recently been discussion about the possibility of miners adopting a hypothetical modified Ethereum client that allows them to essentially accept bribes to make a short reorg of the chain…

I have some doubts about the formula in here

[

Screenshot_2021-07-20-22-20-19-75

720×1600 125 KB

](https://ethresear.ch/uploads/default/original/2X/b/b097d63a7181a81a6bb18471b39a3eccac03732e.jpeg)

-First of all, the formula presented is missing a parameter say “M” to represent the number of groups (committees we have), where the probability P of myopic represents having say “X” malicious such that

P=X/NM

So there must be something wrong in this formula

-True at the end the shuffling algorithm chooses one at random, this could mean to divide the resulting probability by 1/M, but not to execlude M at all; I don’t think things are that simple.

-Bernoulli trials (which the binomial distribution is based on) only have two outcomes (like throwing a coin), but we here have more than 2 groups; it looks like the number of slots was mixed up with the number of groups or maybe the simple example above it.

-It could be more viewed like throwing a dice only with M outcomes (I mean throwing a dice is a special case or example with M=6)

»»»I think there maybe(probably) a known formula or distribution for such probability that I can’t recall now

.

-Another way of viewing it is like u have an NM bits number where u know have exactly X=P

N*M 1s (or 0s), we want to know the probability that when partitioning the number to groups of N contiguous bits, at least N/2 of the X 1s will be in one of those groups.

Till we are able to derive a general formula (or someone remind us of known one from the literature), please follow this simple examples with me to realize the error in the equation when we have more than 2 groups; ie. M≥3

.

-Let M=3, N=5 (15 attestor divided into 3 groups of 5 each)

-say X=4 (we have 4 malicious/myopic persons) where 0.25≤(P=4/15)≤0.33

P~=0.2666…

.

The 4 malicious (consider them persons, ie identity matters let’s call them A,B,C,D)

Have 3^4=81 ways to be distributed over the 3 groups (each has 3 choices to one of the groups, and in general these choices are indep as long as N≥X)

-Possible outcomes are:

4,0,0 ==⟩ can happen in 3 ways

(which of the 3 groups they will be in)

3,1,0 ==⟩ can happen in 43

2=24 ways:

Pick each of the 4 be the single one and choose its group in 3 different ways, the remaining have 2 choices of the 2 remaining groups; in detail

ABC,D,0/ABC,0,D/0,ABC,D/0,D,ABC/D,ABC,0/

D,0,ABC

Then repeat for

ABD,C,0

BCD,A,0

ACD,B,0

.

Till now prob =(3+24)/81=27/81=1/3

That’s larger than initial probability (if we re-divide by3 for the shuffler selection we get 1/9 still not the same as the presented formula).

We can check the rest of options (less than 50% of N) to be sure the enumeration of all cases add up to 81 so we are not wrong.

.

-2,2,0 ==⟩3*6=18

-Divide them into 2 groups in 3 ways?

AB,CD/AC,BD/AD,BC

that’s it

-now arrange the 3 partitions (these two& zero)in the 3 groups in 3!=6 ways

2,1,1==⟩ 66 =36

1st two& their group in 12

3/2=6ways

The arrangement in the groups in 3!=6 ways

AB,C,D/AB,D,C/C,AB,D/C,D,AB/D,AB,C/D,C,AB

AC,B,D/AC,D,B

AD,B,C/AD,C,B

BC,A,D/BC,D,A

BD,A,C/BD,C,A

CD,A,B/CD,B,A

.

Total=3+24+18+36

=81 ✓

If u find this example hard to follow check the case when X=3 (P=3/15=0.2)

.

A,B,C

A(1,2,3),B(1,2,3),C(1,2,3) 27 ways

3,0,0 ⟩ 3 ways

Prob(≥50%)=3/27=1/9

check the rest:

2,1,0 ⟩ 33

2=18ways

1,1,1⟩ordering=3!=6ways

total=3+6+18=27 ✓

If u get it now, check the case where P=1/3, ie X=5 like N, we have the possibilities:

5,0,0 ==⟩ could happen in 3 ways

4,1,0 ==⟩ 30

5 ways to choose the single one* 3!=6 to arrange

3,2,0 ==⟩60

54/2=10 to choose 3 out of 5, then * 3!=6 to arrange

3,1,1 ==⟩60

5

4/2=10 to choose 3 out of 5, then * 3!=6 to arrange

2,2,1 ==⟩90

5 to choose the single one, * selecting 2of4 43/2=6, /2 divided by 2 for the order of the 2 elements partitions doesn't count, 3!=6; ie 5

6

6/2=90

Total no of ways $=3^5=243$

Prob(≥50%)= (3+30+60+60)/243 =153/243 =51/81 … ≥ 0.5

If we divide by 3 again for the o/p of the shuffling is only 1 committee

51/243=0.209

Now let's get back to the formula in the article & substitute with N=5 for both values of P to see the difference in the results:

When X=3, p=0.2

the summation has only one term

Prob=$(0.2)^3$ $(0.8)^2$

10

=8

$64/10^4$= 0.0512

»»»» Does NOT equal 1/9

If we tried to divide by 1/3 (maybe this is his point)

1/27~0.037037…

still NOT the same

.

When X=4, P=4/15, 1-P=11/15

The summation has 2 terms 4,1 and 3,2

Prob= $(4/15)^4$

$(11/15)5 + (4/15)^3$

$(11/15)^{2*}(54/2)$

$=(4^3/15^5)11$

5[4+11

2]

=(6411

26)/$(3*15^4)$

=18,304/151,875

=0.12052

»»»»» Does NOT equal 1/3

If we tried to divide by 1/3 (maybe this is his point)

1/9~0.11111…

still NOT the same

When X=5, P=1/3, 1-P=2/3

The summation has 3 terms 5,0 & 4,1 & 3,2

Prob= $(1/3)^5 + (1/3)^4$

$(2/3)5 + (1/3)^3$

$(2/3)^{2*}(54/2)$

$=(1/3)^5$ [1+ 2

5 + 4

10]

=51/243

Only in this case when X=N, the probability is the same as after selecting a group at random, but this is a special case; and yet the probability is not very small though

.

I know I didn't derive a fixed formula or recall an existing one from the literature yet, but at least this to point out the written one is not accurate?