Hello, ethresearch community. I will state here some problem, present a solution, and am asking for review, comments and references on similar approaches!

So, question is the following: suppose I have an identity system, in which the “validity” or “reliability of sybil-resistance” of an individual voter is a continuous parameter. Typical case could be proof-of-participation in some online community: while you can indeed create multiple identities, you will need to spread your efforts between them.

(*) The (weak) sybil-resistance assumption is thus: for an individual human with identities $1, ..., n$

the validity/participation parameters satisfy $x_1 + ... + x_n \leq 1$

(and could be greater for some extraordinary commited humans, but not too much).

Suppose also, that each identity holds some amount of voting token.

The required schema should satisfy the following:

(1) Collapses to quadratic voting in case where every human has 1 identity.

(2) Splitting identities under assumption (*) does not increase voting power.

Formula is the following: each identity with validity parameter x

and spending y

of voting token on some issue gets the vote impact $\sqrt{xy}$

.

The proof is straightforward:

Suppose that a human has Y

of voting token that they are willing to commit to an issue, and has identities $1, ..., n$

, with validity factors $x_1, ..., x_n$

such that $x_1 + ... + x_n = 1$

.

Then, they must maximize the following: $\sqrt{x_1 y_1} + ... + \sqrt{x_n y_n} \rightarrow \text{max}$

, under assumption $y_i > 0 \forall i, y_1 + ... + y_n = Y$

.

This is easy to maximize: substitute $x_i = a_i^2, y_i = b_i^2$

. Denote $\mathbf{a} = (a_1, ..., a_n), \mathbf{b} = (b_1, ..., b_n)$

. Then, we are actually maximizing the value $\langle \mathbf{a} , \mathbf{b} \rangle$

under assumption $|\mathbf{b}|^2 = Y$

. This is achieved when $\mathbf{b} = \sqrt{Y}\mathbf{a}$

, and the value is $\sqrt{Y}$

, so the human does not improve their voting power by distributing identity.

Questions:

1. Does this work? Is my reasoning correct?
2. Is there any research in this direction?
3. Are there any applications using proof of a participation and this schema?

Considering (3), I disclose that I’m trying to create governance protocol for some gaming project, but I think it should be a natural construction in general anytime there is some continuous notion of “reliability” of identity, or reputation system.