

灯台と ABC プレースの物理的ゼロ知識証明

Physical Zero-Knowledge Proofs for Lighthouses and ABC End View

深澤拓朗 *
Takuro Fukasawa

真鍋義文 †
Yoshifumi Manabe

キーワード ゼロ知識証明, カードベース暗号, パズル, 灯台, ABC プレース

あらまし

ゼロ知識証明とは、証明者が検証者に対して、ある命題が真であることを、真であること以外の情報を漏らさずに証明する手法である。ゼロ知識証明は、カードなどの道具を用いることで、物理的に実装することができる。これまで、数独やカックロなどの様々なペンシルパズルの物理的ゼロ知識証明プロトコルが提案されてきた。本稿では、灯台と ABC プレースという 2 つのペンシルパズルの物理的ゼロ知識証明プロトコルを提案する。

灯台のグリッドは、船を配置することができる白マスと、灯台と呼ばれる黒マスによって構成される^[1]。灯台が照らす範囲は水平・垂直方向にあるマス全てであり、範囲内に船や別の灯台があっても端まで照らすことができる。図 1 に、灯台の例題とその答えを示す。プレイヤーは、以下に示す 4 つのルールに従って、船を配置する必要がある。

1. 船は灯台の縦、横、斜めに隣接してはいけない。
2. 船は少なくとも 1 つの灯台に照らされていなければならない。
3. 灯台は書かれた数字と同じ数の船を照らしていなければならない。
4. 船同士は互いに縦、横、斜めに隣接してはいけない。

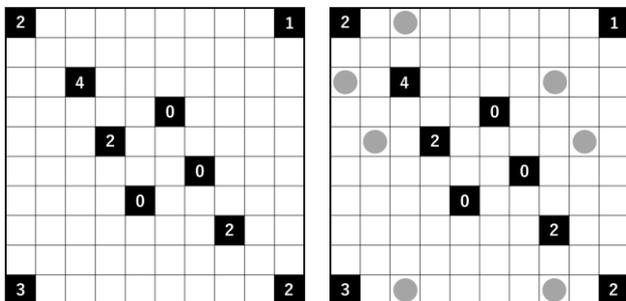


図 1 10 × 10 の灯台の例題とその答え

ABC プレースは、正方形のグリッドに文字を配置していくペンシルパズルである^[2]。図 2 に、ABC プレースの例題とその答えを示す。プレイヤーは、以下に示す 2 つのルールに従って、文字を配置する必要がある。

1. 文字は行および列に重複なく 1 つずつ入っていないといけない。
2. グリッド外の文字と、その行および列の中で最もグリッド外の文字に近い位置にある文字が一致していなければならない。

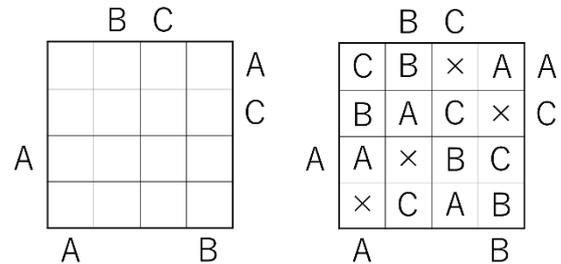


図 2 4 × 4 の ABC プレースの例題とその答え

参考文献

- [1] Cross+A: “Cross+A :: Puzzles”, <http://www.cross-plus-a.com/puzzles.htm#Lighthouses>, 2021 年 11 月 15 日参照
- [2] Cross+A: “Cross+A :: Puzzles”, <http://www.cross-plus-a.com/puzzles.htm#EasyAsABC>, 2021 年 11 月 26 日参照

* 工学院大学 情報学部 システム数理学科, 東京都新宿区西新宿 1-24-2, Faculty of Informatics, Kogakuin University, 1-24-2, Nishishinjuku, Shinjuku-ku, Tokyo, j31234@ns.kogakuin.ac.jp

† 工学院大学 情報学部 システム数理学科, 東京都新宿区西新宿 1-24-2, Faculty of Informatics, Kogakuin University, 1-24-2, Nishishinjuku, Shinjuku-ku, Tokyo, manabe@cc.kogakuin.ac.jp