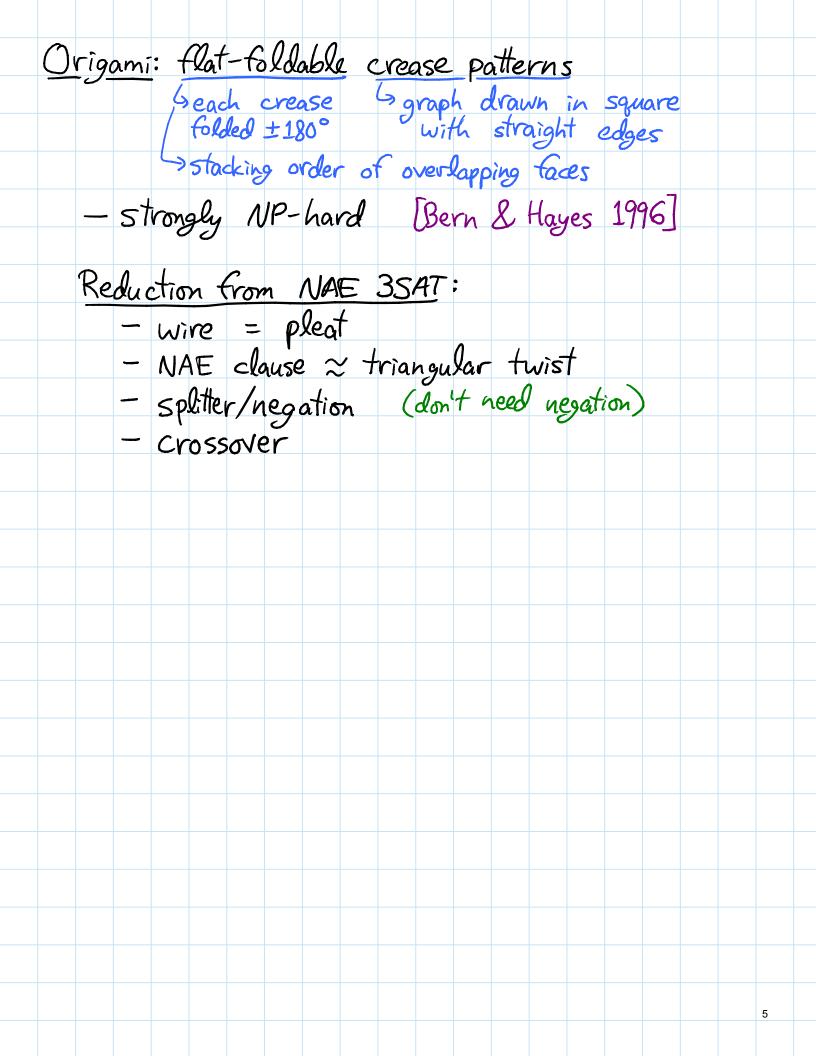
| Ph | utl | sall | 1 (| Phi | los | oph | er ¹ | S | Foot | fbal | \mathcal{U} | ſ | Cor | wa | 43 | | | | |
|------------|---------------|------|---------------|-------------|-------------|------------|-----------------|-----------|------------|-----------|---------------|--------|----------------|-------------|-------------|-------|-------|------|------|
| ' — | | 97 | Q (| whi | te | st | on | 2 (| bal | $U)_1$ | n | ran | y. | bla | ck | sto | nes | (me | en) |
| | - | mo | ve | Ξ | P. | lac | e i | rev | J & | olac | k | st | 574 | , | | | | | |
| | | | | OR | | kic | k t | he tim | 60 | | الح | J J | um 1. | Ping | 3 b | norī | zon | tall | 4 |
| | | | | | | | | | ally ly | | | | | | | | , + | | |
| | _ | 900 | al: | V | eac | h | ορ | por | ient | 15 | Sì | de | バビ ム | siH | d | all | 1 | | |
| | | | | | | | | | | | | | | | | - | | | |
| | | _ | | • | | | | |)ere | | | | २०१ | 9 J | | | | | |
| | | | | | | | | | ON P | | | | | | 1. | | | | |
| | _ | N | - C | omp | oxe | re | 16 |) (| lec | ide ma | r | noi | 27 | <u> </u> | 1. (L : | -67 | | | |
| | | _ | rea | Juc | tion | + | rom | | 3SA | T | De | mai | ne, | De | mail | ne, E | IPPĒ | ein | 3090 |
| | | | | | | | | | | | | , | | | | | '' | | |
| | \mathcal{C} | hec | ke | <u>rs</u> : | | | | 0 | 1 | | | | Γ+- | 1 | 0 | _ | 7 | - 1 | |
| | | | Ex | PTJ | <u>C</u> ME | -C | omp | slet | 20 | | . 0 | | _Hra | euk | ex, (| sypc | 14, J | ohn: | son, |
| | | | ma | re- | in- | e T | 15 | -010 | oly | non ~ | iial 0 | . la | ٥ | oha ocid | eter | 108 | sha | 197 | ره |
| | | | \Rightarrow | E | lex | * * | Pa | th | ve Pr | المح | len | J | P | A1 / I | g | | | | |
| | | | | | 01 | | \ | | l T | | | | | | | | | | |
| | | | | | | | | | | | | | | | | • | | | |

```
Cryptarithms/alphametics [Madachi 1979]
   - given formula x+y=z with each number
     written in base 6 & encoded with "letters" by
   unknown bijection between {0,1,..., b-1} & letters - goal: feasible? / recover bijection
   - strongly NP-complete [Eppstein 1987]
  Reduction from 3SAT:
      - variable gadget:
        -b_i = 2a_i
                                C = carry(y_i + y_i) \in \{0, 1\}
         -v_{i} = 26i + C
           = 4a_i + C = C \pmod{4}
        -d_i = 2c_i + C
        -e_i=d_i+1+C
             =2c_{i}+1+2C
        -\overline{V_i} = d_i + e_i
              =4c_{i}+1+3C
              = 3C+1 = 1-C \pmod{4}
      - clause gadget:
         -g_i = \lambda f_i
         -h_i = 29i + 20,13
              =4f_{i}+\{0,1\}
         -t_i = h_i + 1 + \{0, 1\}
              =4f_{i}+1+\{0,1,2\}
              =4f_{1}+\{1,2,3\}
         -V_{a}+V_{b}+V_{c}=t_{\bar{i}}=\{1,2,3\}\pmod{4}
```

```
Simplified reduction from 1-in-35AT:
   - variable gadget: just vi. no Vi (monotone)
   - clause gadget:
      -g_i = 2f_i
      - h; = 2gi
            = 4f;
      -t_i = h_i + 1
           = 44,+1
      - V_0 + V_b + V_c = t_i
                   = 4fi+1 = 1 (mod 4)
3SAT solvable > cryptarithm solvable:
   - distinguish ambincindin... by value mod 128
   -e.g. V_i = 8 \pmod{128} if true
             = 9 (mod 128) if false
         a: = {2, 34, 66, 98} (mod 128)
   - set \lfloor V_i / 128 \rfloor & \lfloor \overline{V_i} / 128 \rfloor \in [0, (2n)^3]
      such that distinct sums of triples
     [Bose & Chowla 1959]
   - easy proof of polynomial range: (based on trees)
      - if < i set by induction. Vi must avoid
         V_j + V_k + V_e - V_m - V_p \sim (2n)^5 choices
      >> (2n)5 suffices
   ⇒ strongly NP-hard
```



Vertex-disjoint paths:
- in a graph [Lynch 1975] — in a planar graph [Lynch 1975] - in a rectangle with all spots filled [Adcock, Demaine, Demaine, O'Brien, Reidl, Sánchez Villaamil, Sullivan 2014] - use terminals as obstacles - neighboring terminal pairs can just connect OR fill some uncovered space - issue 1: must have even-parity fill regions - issue 2: clause path may be absent! -> more parity trouble -> add row - issue 3: gadget width is odd parity > won't connect to split > add column - issue 4: crossing true or false line gadgets = Zig-zag Numberlink [Loyd 1897; Nikoli] - classic Numberlink also NP-complete [Kotsuma & Takenaga 2010]

6.890 Algorithmic Lower Bounds: Fun with Hardness Proofs Fall 2014

For information about citing these materials or our Terms of Use, visit: http://ocw.mit.edu/terms.