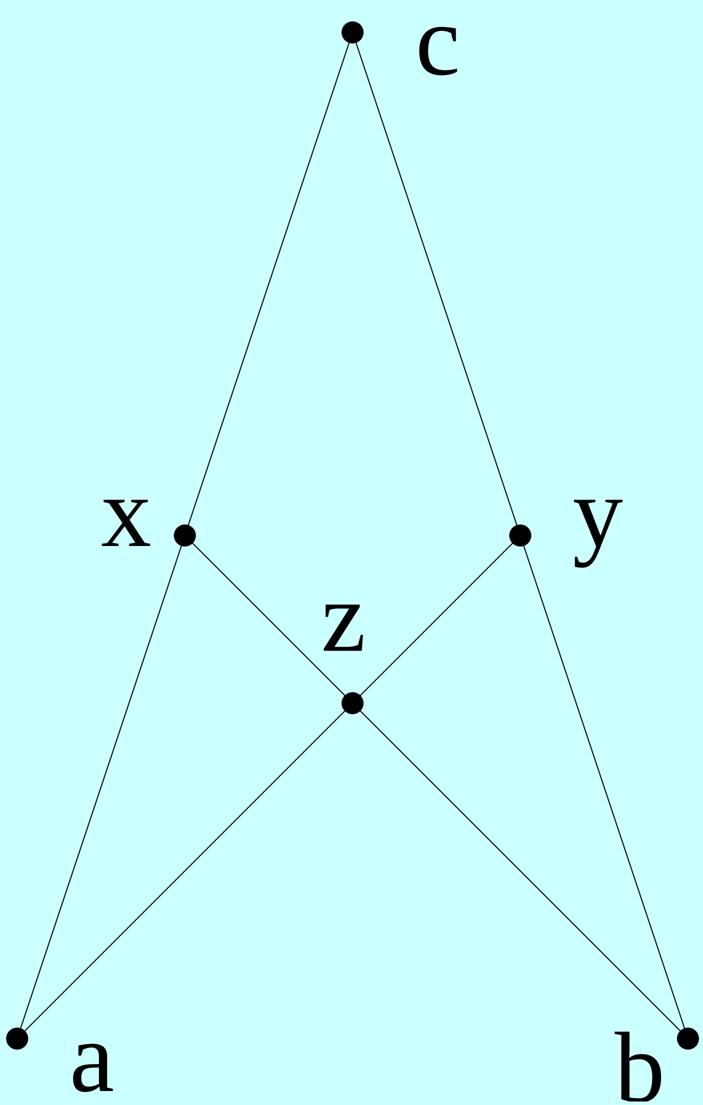
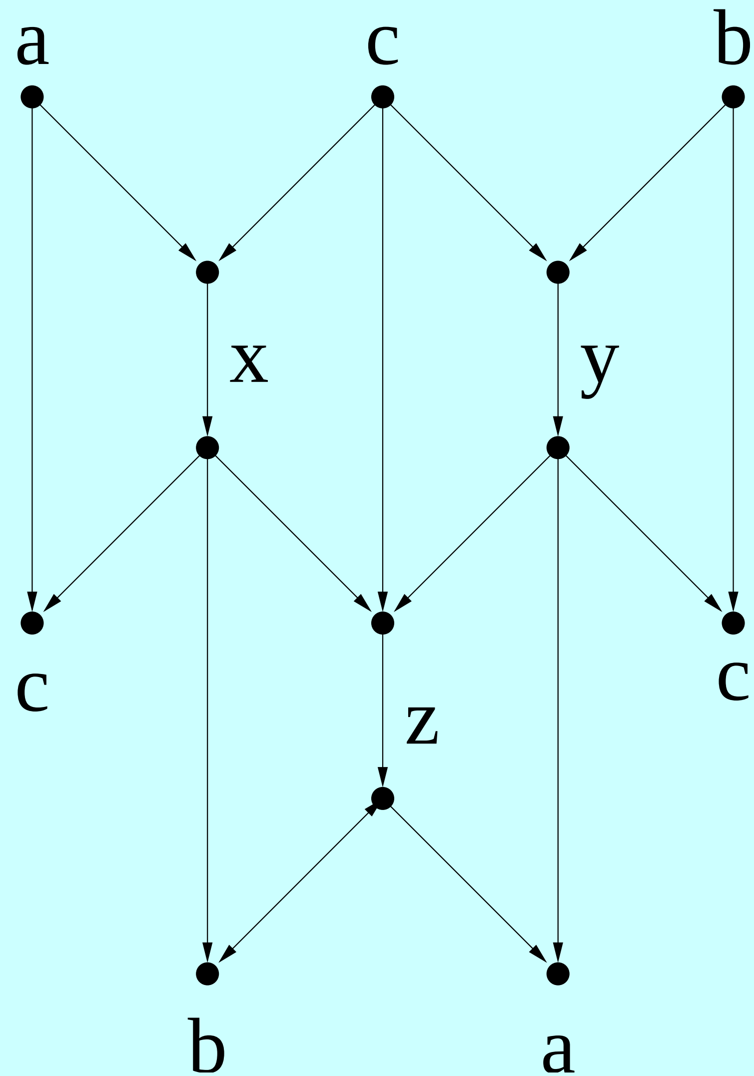
Is network coding undecidable?

Randall Dougherty

(Center for Communication Research, La Jolla)

This talk gives an outline of a proof (with two holes at present) that network coding solvability is undecidable, which proceeds by reducing a known group-theoretic problem to it.


c
x
y
z
a
b


a
c
b
x
y
c
z
c
b
a

General solution for this network

$$x' = a' * c$$

$$y' = c * b'$$

$$z' = a' * c * b'$$

where * is a group operation, and v' is a permutation of v.

Message variables

Word variables:

$$a_1, a_2, a_3, \ldots$$

Auxiliary variables:

$$g_1, g_2, g_3, \ldots$$

Initial products

$$a'_1 * a'_2, \quad a'_2 * a'_3, \quad \ldots$$

(using interlinked copies of the previous network)

$\boxed{\textbf{Triple products}}$

$$p_{i,k,j}(g_i) * a'_k * q_{i,k,j}(g_j)$$

If we have distinct messages r, s, t and edges x, y such that

$$x' = r' * t' \qquad \text{and} \qquad y'' = s'' * t'',$$

then we can add edges and demands to the network so as to enforce that the mapping $t' \mapsto t''$ is a group automorphism.

$$x, y \longrightarrow w$$

$$w, r \longrightarrow s$$

$$w, s \longrightarrow r$$

If we have distinct messages r, s, t and edges x, y such that

$$x' = r' * t' \qquad \text{and} \qquad y'' = t'' * s'',$$

then we can add edges and demands to the network so as to enforce that the mapping $t' \mapsto t''$ is a group antiautomorphism.

$$x, y \longrightarrow w$$

$$w, r \longrightarrow s$$

$$w, s \longrightarrow r$$

Triple products

$$p_{i,k,j}(g_i) * a'_k * q_{i,k,j}(g_j)$$

Triple products

$$\psi_{i,k,j}(g_i'^{-1}) * a_k' * \phi_{i,k,j}(g_j')$$

Triple products

$$\psi_{i,k}(g_i'^{-1}) * a_k' * \phi_{k,j}(g_j')$$

Triple products

$$\psi_k(g_i'^{-1}) * a_k' * \phi_k(g_j')$$

Triple products

$$g_i'^{-1} * a_k' * \phi_k(g_j')$$

Hole #1

$$g_i'^{-1} * a_k' * g_j'$$

Creating a network edge to represent a group word

To represent the word

$$w = a_1 a_2 a_1^{-1}:$$

add an edge x such that

$$g_1^{-1} * a_1 * g_2, \quad g_2^{-1} * a_2 * g_3, \quad g_4^{-1} * a_1 * g_3 \quad \longrightarrow \quad x,$$

$$g_1, x, a_1, a_2 \longrightarrow g_4.$$

Then

$$x' = g_1^{-1} w g_4.$$

Enforcing an identity

To enforce the identity

$$w \equiv e,$$

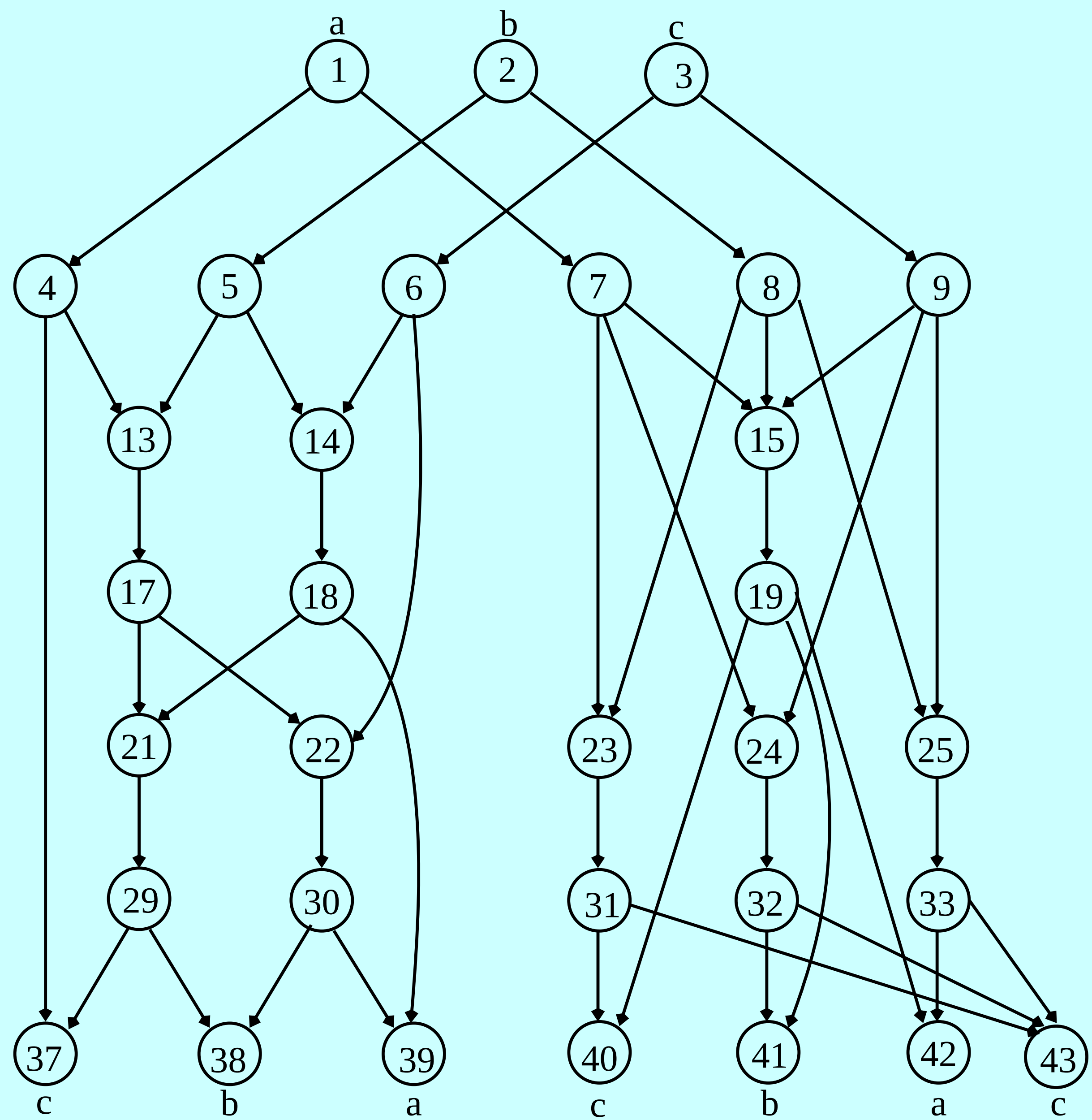
create an edge x for $g_1^{-1} w g_k$ and put in the demand

$$x, g_1 \longrightarrow g_k.$$

Enforcing failure of an identity

To enforce the non-identity

$$w \not\equiv e,$$


a
b
c
1
2
3
4
5
6
7
8
9
13
14
15
17
18
19
21
22
23
24
25
29
30
31
32
33
37
38
39
40
41
42
43
c
b
a
c
b
a
c

Enforcing failure of an identity

To enforce the non-identity

$$w \not\equiv e,$$

use a redundant form of the preceding network (each of a,b,c here becomes a tuple of messages, one for each word variable) and feed in side information at the bottom from the edge(s) representing $g_1^{-1} w g_k$ (and from the auxiliary variables g_1 and g_k).

Rhodes' problem

The identity (Tarski-Mal'cev) problem for finite groups: Does the fact that identities $w_1 \equiv e, \ldots, w_k \equiv e$ hold in finite group G imply that the identity $u \equiv e$ also holds in G?

The pieces previously described allow us to reduce an instance of this problem to a instance of the network coding solvability problem.

$\boxed{\textbf{Hole \#2}}$

It is currently open whether Rhodes' problem is undecidable.

What is known

The identity problem for semigroups is undecidable. (Murskii, 1968)

The identity problem for groups is undecidable. (Kleiman, 1979)

The identity problem for finite semigroups is undecidable. (Albert-Baldinger-Rhodes, 1992)

Though this is not a complete proof, it might make it more plausible that network coding solvability is undecidable.

Can something similar be said about matroids and secret-sharing?

The End.