Sucesiones-F, ciclos hamiltonianos en el hipercubo y problemas difíciles

Candidato a doctor: **Israel Buitrón-Dámaso**
Directores: **Guillermo Morales-Luna, Feliú Salgols-Troncoso**

28 de septiembre de 2018

Revisamos los avances realizados en el trabajo de tesis hasta el momento. La propuesta inicial presentada en el protocolo de investigación doctoral se centró en el estudio de protocolos de autenticación, específicamente las pruebas de conocimiento nulo (ZKP's), basados en problemas difíciles de la teoría de grafos. Sin embargo, este enfoque fue modificado. El análisis del problema de gráficas considerado originalmente nos mostró la inviabilidad para su aplicación práctica en los protocolos criptográficos, por lo que el estudio se centró al área de la teoría formal de gráficas.

Cada hipercubo es una gráfica hamiltoniana y el número de ciclos hamiltonianos tiene un crecimiento doblemente exponencial. Cualquier ciclo hamiltoniano en el hipercubo se describe mediante una secuencia cuyas entradas son los índices de las direcciones base recorridas a través del ciclo. Estas secuencias numéricas se llaman sucesiones-f (suc's-f). Mediante de transformaciones elementales, por ejemplo. rotación de secuencias, reflexión de secuencias, y algunos otros, las suc's-f se clasifican en clases de equivalencia. Hemos definido un representante canónico de cada clase. Existe un gran número de clases de ciclos en el hipercubo.

El Código de Gray es la suc-f mínima lexicográfica y es particularmente interesante debido a varias propiedades. A partir de los representantes de las suc's-f, hemos introducido varias transformaciones. Para cada transformación de este tipo, hemos construido una gráfica de trayectoria particular: los vértices son los representantes de las suc's-f y las aristas resultan de la transformación, donde un vértice y su vértice transformado forman una arista.

Al considerar varias transformaciones, podemos considerar la unión de las (aristas) gráficas de trayectorias correspondientes. Estás son gráficas enormes doblemente exponenciales. Describiremos varias transformaciones: el trébol, el trébol invertido, el hongo y el hongo invertido.

Así surgen varios problemas, por ejemplo. ¿cuáles son los conjuntos de transformaciones mínimos que producen gráficas de trayectorias conexas?, o para una transformación dada, ¿cuál es el número de componentes conexas en el gráfico de trayectoria? Hemos diseñado varios algoritmos para la aplicación eficiente de transformaciones y para responder a varios problemas de decisión, así como

para generar aleatoriamente suc's-f con el fin de verificar problemas de conexidad y accesibilidad, en ambas versiones: decisión y búsqueda. Hemos, también, construido una biblioteca de C que implementa esos algoritmos. Esta biblioteca es compatible con el sistema de compilación GNU, lo que permite una fácil instalación, portabilidad y fácil uso de las funciones.