Universidad Nacional Autónoma de México

Posgrado en Ciencia e Ingeniería de la Computación

Códigos sobre Grupos Cuánticos Finitos y sus Rangos Combinatorios

T E S I S

QUE PARA OPTAR POR EL GRADO DE

DOCTORA EN CIENCIAS
(COMPUTACIÓN)

PRESENTA:

MAYRA LORENA DÍAZ SOSA

TUTOR:

DR. VLADISLAV KHARTCHENKO

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLÁN

MÉXICO, D.F., MARZO DE 2015.

Tesis elaborada con apoyo del Consejo Nacional de Ciencia y Tecnología (CVU 205912) y de la Universidad Nacional Autónoma de México (Proyecto PAPIIT IN-112913, *Estructuras algebraicas relacionadas a los grupos cuánticos*).

Agradecimientos

La conclusión de mis estudios doctorales no habría sido posible sin diversos apoyos. Mi más profundo agradecimiento:

A Dios, que día a día me bendice.

A mi madre, María Concepción Sosa Tuñón, quien me ha colmado de amor desde el primer día en que mis ojos vieron la luz y brindado siempre el aliento que he necesitado para seguir adelante.

A mi esposo, Víctor Manuel Rangel Cortés, por su comprensión y por alentarme a enfrentar nuevos retos.

A la Universidad Nacional Autónoma de México, por convertirse en mi casa y brindarme la oportunidad de crecer en ella no sólo en lo académico, sino también en lo profesional.

A mi asesor, el Dr. Vladislav Khartchenko, por su confianza, paciencia y dedicación.

Al Consejo Nacional de Ciencia y Tecnología, por la beca otorgada para realizar mis estudios.

Y a todos aquellos quienes con paciencia y cariño me acompañaron en mi andar a lo largo de esta aventura académica.

Mayra Lorena Díaz Sosa.

Resumen

La Teoría de Códigos tuvo sus orígenes en el escenario de los campos finitos. Sin embargo, el estudio de códigos sobre anillos finitos ha cobrado interés en los últimos años debido a que la Extensión del teorema de MacWilliams, resultado fundamental para establecer la equivalencia entre códigos dentro de la teoría clásica, se verifica en este contexto si y sólo si el anillo es de Frobenius. Aunque estos anillos guardan una estrecha relación con los grupos cuánticos, hay pocas investigaciones sobre códigos construidos bajo estas estructuras algebraicas y, menos aún, que estudien la factibilidad computacional de su implementación. Para emplear un grupo cuántico como alfabeto de un código es necesario introducir la estructura algebraica a la computadora en un número finito de pasos conocido como rango combinatorio. El objetivo de la presente investigación es determinar el rango combinatorio de la versión multiparamétrica del grupo cuántico de Lusztig pequeño $u_q\left(\mathfrak{so}_{2n+1}\right)$ de tipo B_n. Mediante el Teorema de Heyneman-Radford y la fórmula explícita para el coproducto del grupo cuántico de Drinfeld-Jimbo $U_q\left(\mathfrak{so}_{2n+1}\right)$ se obtiene una proposición de la que se desprende el rango combinatorio de este caso particular. Los resultados revelan que se requieren sólo $\lfloor \log_2 (n-1) \rfloor + 2$ pasos para introducir un alfabeto basado en esta estructura algebraica a la computadora, un número muy pequeño desde la perspectiva computacional. De reproducirse la metodología expuesta en este estudio para otros grupos cuánticos, podría determinarse la factibilidad de su implementación como alfabetos de un código, así como generarse antecedentes que den paso a la creación de mecanismos para la codificación y decodificación de información en este contexto.

Palabras clave: anillos de Frobenius, identidades de MacWilliams, extensión del teorema de MacWilliams, teorema de Heyneman-Radford, elementos primitivos torcidos, base PBW.

Índice general

Introducción

En la actualidad, es posible la transmisión casi inmediata de mensajes enviados a través de dispositivos electrónicos sujetos a canales con presencia de ruido, como son cables de cobre, cables de fibra óptica, el almacenamiento en dispositivos móviles como memorias USB y celulares, entre otros. Sería deseable que aunque los mensajes enviados por estos medios fueran distorsionados durante su transmisión, fueran recibidos y recuperados de algún modo. La estrategia básica para la corrección de errores consiste en añadir redundancia el mensaje (codificación) para que los errores puedan ser detectados de manera eficiente y finalmente corregidos (decodificación).

Al área de las matemáticas que se encarga de estudiar cómo asegurar la integridad de un mensaje que ha sido enviado a través de un canal en presencia de ruido se le conoce como Teoría de Códigos. Ésta comenzó con los estudios de Claude Shannon en 1948 (véase [62]) y desde entonces ha despertado el interés tanto de matemáticos como de estudiosos de las ciencias de la computación, quienes han hecho gran uso de álgebra, cálculo combinatorio y, primordialmente, álgebra lineal sobre campos finitos para su desarrollo.

En la teoría clásica, hay dos resultados de particular importancia conocidos como las identidades de MacWilliams y la Extensión del teorema de MacWilliams. Las identidades de MacWilliams relacionan el enumerador del peso de Hamming de un código lineal con aquel que corresponde a su código dual. Estas identidades encuentran amplia aplicación, especialmente en el estudio de códigos autoduales. Por su parte, la Extensión del teorema de MacWilliams aborda la noción de equivalencia entre códigos. Dos códigos lineales son equivalentes si existe una transformación monomial que defina un isomorfismo entre ellos que preserve el peso de Hamming. Mostrar que una transformación monomial define tal isomorfismo no es tan complejo como el problema inverso, esto es, mostrar si todo isomorfismo entre códigos lineales que preserve el peso de Hamming se extiende a una transformación monomial. En [51], MacWilliams demostró que este es el caso cuando se trata de campos finitos.

A pesar de que en sus inicios la Teoría de Códigos yace en el contexto de los campos finitos, ésta ha comenzado a desarrollarse desde hace ya algunos años sobre anillos finitos, luego de descubrirse que códigos aparentemente no lineales en realidad lo son sobre el anillo $\mathbb{Z}_4$. Ejemplos de ello son los trabajos de Calderbank, Pless y Qian ([8], [57] y [56], respectivamente). De hecho tanto las identidades de MacWilliams como la Extensión del teorema de MacWilliams son generalizables a códigos lineales sobre anillos finitos. Dentro de los anillos finitos, los anillos de Frobenius resultan de particular interés debido a que son la clase más larga sobre la cual es válida la Extensión del teorema de MacWilliams.

Por otra parte, los anillos de Frobenius se encuentran estrechamente ligados a los grupos cuánticos finitos, estructuras algebraicas modernas cuyo marco teórico son las álgebras de Hopf. Recientemente, esta relación ha abierto nuevos caminos a la Teoría de Códigos. Los artículos de Cuadra, García-Rubira, y López-Ramos ([13] y [14]), así como el de Xiaoping [81], dan testimonio de ello.

Para emplear estructuras algebraicas distintas a las clásicas en la construcción de códigos es preciso establecer primero la factibilidad de su uso como alfabeto en cuanto al número de pasos requeridos por la representación combinatoria ordinaria ya que si éste es, computacionalmente hablando, grande entonces la implementación del código en la práctica no resultaría viable. El objetivo de esta tesis es determinar el rango combinatorio de la versión multiparamétrica del grupo cuántico conocido como grupo cuántico de Lusztig pequeño $u_q(\mathfrak{so}_{2n+1})$ de tipo B_n sobre campos finitos. El estudio revela que se requieren $\lfloor \log_2(n-1) \rfloor + 2$ pasos para introducir a una computadora un alfabeto basado en esta estructura algebraica particular (resultado publicado en [33]).

Cabe destacar que la gran mayoría de los artículos sobre grupos cuánticos versa sobre campos de característica 0, todos ellos infinitos. Sin embargo, al requerir la Teoría de Códigos del uso de estructuras algebraicas finitas, es preciso abordar los conceptos de los grupos cuánticos sobre campos finitos.

En el Capítulo 1 se describe la caracterización de los anillos de Frobenius bajo la teoría de caracteres. Se abordan también las similitudes entre una álgebra de Frobenius y un anillo de Frobenius finito. Asimismo, se hace una breve presentación de conceptos fundamentales de la Teoría de Códigos y se presentan las identidades de MacWilliams, así como la Extensión del teorema de MacWilliams.

Luego, en el Capítulo 2, se hace una introducción a las álgebras de Hopf y algunos conceptos fundamentales asociados. Se presenta un resultado bien conocido que indica que toda álgebra de Hopf de dimensión finita es de Frobenius. Esta relación, y el hecho

de que los grupos cuánticos son casos particulares de álgebras de Hopf finitas, conecta a los anillos de Frobenius con los grupos cuánticos.

En el Capítulo 3 se hace una introducción al tema de los grupos cuánticos en la que la noción de álgebra universal envolvente cuántica para cualquier álgebra de Lie es definida a través de generadores y relaciones basadas en el concepto de operaciones cuánticas de Lie. En este capítulo también se aborda el concepto de rango combinatorio.

En el Capítulo 4 se hace una descripción del grupo cuántico $U_q^+(\mathfrak{so}_{2n+1})$. Se muestran también las relaciones del álgebra cuántica de Borel y sus generadores de Poincaré Birkhoff Witt.

Por último, en el Capítulo 5, se calcula el rango combinatorio de la versión multiparamétrica del grupo cuántico de Lusztig pequeño $u_q(\mathfrak{so}_{2n+1})$ de tipo B_n para el caso en q tiene un orden finito multiplicativo t mayor a 4.

Finalmente, se presentan las conclusiones del estudio y en el apéndice se presenta la cuantificación de $\mathfrak{so}_{2n+1}$, para lo cual se hace una revisión del caso del kernel de Frobenius-Lusztig de tipo A_n.

Capítulo 1

Anillos de Frobenius y la Teoría de Códigos

Las identidades de MacWilliams y la Extensión del teorema de MacWilliams son de gran importancia no sólo en un sentido teórico sino también práctico. De acuerdo con Honold [27], comprender cuándo un tipo de anillo satisface alguna versión del teorema de equivalencia de MacWilliams, por ejemplo, asegura a los desarrolladores de códigos que, tan pronto como se adopten dichos anillos, la singularidad de sus resultados se convertirá en algo sencillo de verificar puesto que la existencia de códigos equivalentes los reducirá a casos más tratables. Ello resulta una tarea de vital importancia, por ejemplo, cuando se trata de patentar un sistema de codificación.

Sobre campos finitos, las demostraciones de las identidades de MacWilliams y de la Extensión del teorema de MacWilliams hacen uso de la teoría de caracteres. En particular, los campos finitos $\mathbb{F}$ poseen la propiedad de que sus caracteres $\widehat{\mathbb{F}}$ forman un espacio vectorial sobre $\mathbb{F}$ y $\widehat{\mathbb{F}} \cong \mathbb{F}$ como espacios vectoriales. Estas demostraciones también funcionan sobre un anillo finito R con la propiedad de $\widehat{R} \cong R$ como módulos de un sólo lado. Resulta ser que los anillos de Frobenius están caracterizados precisamente por esa propiedad, como se muestra en [25, Teorema 1] e independientemente en [**?**, Teorema 3.10].

1.1. Anillos de Frobenius finitos

En esta sección se abordará la teoría de caracteres de los anillos de Frobenius finitos, mismos que se caracterizan por poseer módulos de caracter libres. Para profundizar en el tema, se sugieren los libros de Lam, [45] y [46].

Dado un anillo finito R, su *radical de Jacobson*, denotado por $\mathrm{rad}\,(R)$ es la intersección de todos los ideales maximales izquierdos de R. $\mathrm{rad}\,(R)$ es él mismo un ideal por ambos lados de R. Un R-módulo izquierdo es *simple* si no cuenta con submódulos propios distintos de cero. Dado un R-módulo izquierdo M, su *soclo* $\mathrm{soc}\,(M)$ es la suma de todos los submódulos simples de M. Un anillo R tiene soclo izquierdo $\mathrm{soc}\,({}_RR)$ y soclo derecho $\mathrm{soc}\,(R_R)$, dependiendo de si a R se le considera un R-módulo izquierdo o derecho. Ambos soclos son ideales por ambos lados, pero pueden no ser iguales (son iguales si R es semiprimo, lo cual, en el caso de anillos finitos equivale a que sean semisimples).

Sea R un anillo finito. Entonces el anillo cociente $R/\mathrm{rad}\,(R)$ es semisimple y es isomorfo a la suma directa de anillos de matrices sobre campos finitos (Wedderburn-Artin):

$$R/\mathrm{rad}\,(R) \cong \bigoplus_{i=0}^{k} M_{m_i}\left(\mathbb{F}_{q_i}\right), \tag{1.1}$$

donde cada q_i es una potencia prima; $\mathbb{F}_q$, un campo finito de orden q; q, una potencia de un primo; y $M_m\left(\mathbb{F}_q\right)$, el anillo de matrices de $m \times m$ sobre $\mathbb{F}_q$.

1.1 Definición ([45], Teorema 16.14)**.** Un anillo finito R es de Frobenius si

$${}_R\left(R/\mathrm{rad}\,(R)\right) \cong \mathrm{soc}\,({}_RR)$$

y

$$\left(R/\mathrm{rad}\,(R)\right)_R \cong \mathrm{soc}\,(R_R).$$

Esta definición aplica de forma general para anillos artinianos. En un teorema de Honold [27, Teorema 2], se demuestra que, para anillos finitos, sólo hace falta uno de los isomorfismos (el izquierdo o el derecho).

Cada uno de los anillos de matrices $M_{m_i}\left(\mathbb{F}_{q_i}\right)$ en (1.1) tiene un módulo izquierdo simple $T_i := M_{m_i\times 1}\left(\mathbb{F}_{q_i}\right)$ que consiste en todas las matrices de $m_i \times 1$ sobre $\mathbb{F}_q$, bajo el producto

de matrices por la izquierda. De (1.1) se sigue que, como R-módulos de izquierda, se tiene el isomorfismo

$$_R\left(R/\mathrm{rad}\left(R\right)\right) \cong \bigoplus_{i=0}^{k} m_i T_i. \tag{1.2}$$

Se sabe que las T_i, $i = 1, \ldots, k$, forman una lista completa de R-módulos izquierdos simples, hasta el isomorfismo.

Debido a que el soclo izquierdo de un R-módulo es la suma de R-módulos izquierdos simples, éste puede expresarse como la suma de las T_i. En particular, el soclo izquierdo de R admite él mismo tal expresión:

$$\mathrm{soc}\left({}_RR\right) \cong \bigoplus_{i=0}^{k} s_i T_i, \tag{1.3}$$

para algunos enteros no negativos $s_1, \ldots, s_k$. Así, un anillo finito es de Frobenius si y sólo si $m_i = s_i$ para toda $i = 1, \ldots k$.

Un *caracter* es un homomorfismo de grupo $\varpi : G \to \mathbb{Q}/\mathbb{Z}$, donde G es un grupo finito abeliano. El conjunto de todos los caracteres de G forma un grupo llamado el grupo caracter $\widehat{G} := \mathrm{Hom}_{\mathbb{Z}}\left(G, \mathbb{Q}/\mathbb{Z}\right)$. Se sabe que $\left|\widehat{G}\right| = |G|$. Los caracteres con valores en el grupo multiplicativo de números complejos distintos de cero pueden obtenerse por medio de la composición con la función exponencial compleja $a \mapsto \exp\left(2\pi i a\right)$, $a \in \mathbb{Q}/\mathbb{Z}$. Esta forma multiplicativa de caracteres se requerirá más adelante en este capítulo.

Si R es un anillo finito y A es un R-módulo izquierdo finito, entonces $\widehat{A}$ consiste en los caracteres del grupo aditivo de A. $\widehat{A}$ es un R-módulo derecho por medio del producto escalar $\left(\varpi r\right)\left(a\right) := \varpi\left(ra\right)$, para $\varpi \in \widehat{A}$, $r \in R$ y $a \in A$. Se llamará al módulo $\widehat{A}$ el *módulo caracter de* A. De manera similar, si B es un R-módulo derecho, entonces $\widehat{B}$ es un R-módulo izquierdo.

1.2 Ejemplo. Sea $\mathbb{F}_p$ un campo finito de orden primo. Definamos a $\upsilon_p : \mathbb{F}_p \to \mathbb{Q}/\mathbb{Z}$ por $\upsilon_p\left(a\right) = a/p$, considerando a $\mathbb{F}_p$ como $\mathbb{Z}/p\mathbb{Z}$. Entonces, υ_p es el caracter de $\mathbb{F}_p$ y cualquier otro caracter ϖ de $\mathbb{F}_q$ es de la forma $\varpi = a\upsilon_q$, para alguna $a \in \mathbb{F}_q$ ya que $\widehat{\mathbb{F}}_p$ es un espacio vectorial unidimensional sobre $\mathbb{F}_p$.

Sea $\mathbb{F}_q$ un campo finito con $q = p^\ell$ para algún número primo p. Sea $\mathrm{tr}_{q/p} : \mathbb{F}_q \to \mathbb{F}_p$ la traza. Definamos a $\upsilon_q : \mathbb{F}_q \to \mathbb{Q}/\mathbb{Z}$ por $\upsilon_q = \upsilon_p$ o $\mathrm{tr}_{q/p}$. Entonces, υ_q es un caracter de $\mathbb{F}_q$ y cualquier otro caracter ϖ de $\mathbb{F}_q$ tiene la forma $\varpi = a\upsilon_q$, para alguna $a \in \mathbb{F}_q$.

1.3 Ejemplo. Sea $R = M_m(\mathbb{F}_q)$ el anillo de matrices de $m \times m$ sobre un campo finito $\mathbb{F}_q$, y sea $A = M_{m\times k}(\mathbb{F}_q)$ el R-módulo izquierdo que consiste en todas las matrices de $m \times k$ sobre $\mathbb{F}_q$. Entonces, $\widehat{A} \cong M_{k\times m}(\mathbb{F}_q)$ como R-módulos derechos. De hecho, dada una matriz $Q \in M_{k\times m}(\mathbb{F}_q)$, podemos definir al caracter ϖ_Q de A por $\varpi_Q(P) = \upsilon_q(\mathrm{tr}(QP))$, para $P \in A$, donde tr es la traza de la matriz y υ_q es el caracter de $\mathbb{F}_q$ definido en el Ejemplo 1.2. El mapeo $M_{k\times m}(\mathbb{F}_q) \to \widehat{A}$, $Q \mapsto \varpi_Q$ es el isomorfismo buscado.

Dada una secuencia corta exacta de R-módulos izquierdos finitos $0 \to A \to B \to C \to 0$, hay una secuencia exacta corta inducida de R-módulos derechos

$$0 \to \widehat{C} \to \widehat{B} \to \widehat{A} \to 0. \tag{1.4}$$

En particular, si se define $\left(\widehat{B} : A\right) := \left\{\varpi \in \widehat{B} : \varpi(A) = 0\right\}$, a lo cual se conoce como *aniquilador*, entonces

$$\left(\widehat{B}, A\right) \cong \widehat{C} \text{ y } \left|\left(\widehat{B} : A\right)\right| = |C| = |B| / |A|. \tag{1.5}$$

En el caso especial en el que $A = R$, R es tanto un R-módulo izquierdo como derecho. Un caracter $\varpi \in \widehat{R}$ induce tanto un homomorfismo por la izquierda como por la derecha $R \to \widehat{R}$ ($r \mapsto r\varpi$ es un homomorfismo izquierdo, mientras que $r \mapsto \varpi r$ es un homomorfismo derecho). El caracter ϖ se llama *caracter generador izquierdo* si $r \mapsto r\varpi$ es un isomorfismo de módulos. En tal caso, el caracter ϖ genera al R-módulo izquierdo $\widehat{R}$. Debido a que $\left|\widehat{R}\right| = |R|$, uno de esos homomorfismos es un isomorfismo si y sólo si es inyectivo y suprayectivo.

De manera independiente Hirano [25] y Wood [77], hallaron una caracterización de los anillos de Frobenius finitos mediante caracteres; un teorema que establece que siendo R un anillo finito las siguientes afirmaciones son equivalentes:

i) R es de Frobenius;

ii) R tiene un caracter generador izquierdo;

iii) R tiene un caracter generador derecho.

Además, demostraron que cuando esas condiciones se satisfacen, todo caracter generador izquierdo es también un caracter generador derecho y viceversa.

Aunque este resultado se publicó en ambos casos hace ya más de una década, a continuación de seguirá la metodología expuesta recientemente por Wood en [80] a quien se deben los resultados de este capítulo a menos que se indique lo contrario.

1.4 Proposición ([10], Corolario 3.6)**.** *Sea R un anillo finito. Un caracter $\widehat{\varpi}$ de R es un caracter generador izquierdo de R si y sólo si* $\ker \varpi$ *no contiene ideales izquierdos de R distintos de cero.*

Demostración. Por definición y dado que $\left|\widehat{R}\right| = |R|$, ϖ es un caracter generador izquierdo si y sólo si el homomorfismo $f : R \to \widehat{R}$, $r \mapsto r\varpi$, es inyectivo. Entonces $r \in \ker f$ si y sólo si el ideal principal $Rr \subset \ker \varpi$. Así, $\ker f = 0$ si y sólo si $\ker \varpi$ no contiene ideales izquierdos distintos de cero. □

1.5 Proposición ([77], Teorema 4.3)**.** *Un caracter ϱ de un anillo finito R es un caracter generador izquierdo si y sólo si es un caracter generador derecho.*

Demostración. Supongamos que ϱ es un caracter generador izquierdo y supongamos que $I \subset \ker \varrho$ es un ideal derecho. Entonces, para toda $r \in R$, $Ir \subset \ker \varrho$, de manera que $I \subset \ker(r\varrho)$, para toda $r \in R$. Pero todo caracter de R es de la forma $r\varrho$ porque ϱ es un caracter generador. Así, el aniquilador $\left(\widehat{R} : I\right) = \widehat{R}$, y se sigue de (1.5) que $I = 0$. Por la Proposición 1.4, ϱ es un caracter generador derecho. □

1.6 Proposición ([79], Proposición 3.3)**.** *Sea A un R-módulo izquierdo finito. Entonces* $\operatorname{soc}\left(\widehat{A}\right) \cong (A/\operatorname{rad}(R)\, A)\widehat{\ }$.

Demostración. Existe una secuencia exacta corta de R-módulos

$$0 \to \operatorname{rad}(R)\, A \to A \to A/\operatorname{rad}(R)\, A \to 0.$$

Tomando módulos caracter, como en (1.4), se produce

$$0 \to (A/\operatorname{rad}(R)\, A)\widehat{\ } \to \widehat{A} \to (\operatorname{rad}(R)\, A)\widehat{\ } \to 0.$$

Ya que $A/\operatorname{rad}(R)\, A$ es una suma de módulos simples, lo mismo es cierto para

$$(A/\operatorname{rad}(R)\, A)\widehat{\ } \cong \left(\widehat{A} : \operatorname{rad}(R)\, A\right).$$

En consecuencia, $\left(\widehat{A} : \operatorname{rad}(R)\, A\right) \subset \operatorname{soc}\left(\widehat{A}\right)$.

A la inversa, $\operatorname{soc}\left(\widehat{A}\right)\operatorname{rad}(R)=0$, ya que el radical aniquila a los módulos simples [15, Ejercicio 25.4]. Así, $\operatorname{soc}\left(\widehat{A}\right)\subset\left(\widehat{A}:\operatorname{rad}(R)A\right)$, y se tiene la igualdad

$$\operatorname{soc}\left(\widehat{A}\right)=\left(\widehat{A}:\operatorname{rad}(R)A\right).$$

El hecho de que $\left(\widehat{A}:\operatorname{rad}(R)A\right)\cong\widehat{(A/\operatorname{rad}(R)A)}$ completa la prueba. □

1.7 Lema. *Sea A un R-módulo izquierdo finito y sea $B\subset A$ un submódulo. Si A admite un caracter generador izquierdo, entonces B también admite un caracter generador izquierdo.*

Demostración. Restrinjamos el caracter generador de A a B. Cualquier submódulo de B en el kernel de la restricción será también un submódulo de A dentro del kernel del caracter generador original. □

1.8 Lema. *Sea R cualquier anillo finito. Definamos $\varrho:\widehat{R}\to\mathbb{Q}/\mathbb{Z}$ como $\varrho(\varpi)=\varpi(1)$, la evaluación en $1\in R$, para $\varpi\in\widehat{R}$. Entonces ϱ es un caracter generador izquierdo y derecho de $\widehat{R}$.*

Demostración. Supongamos que $\varpi_0\neq 0$ tiene la propiedad de que $R\varpi_0\subset\ker\varrho$. Esto significa que para toda $r\in R$, $0=\varrho(r\varpi_0)=(r\varpi_0)(1)=\varpi_0(r)$, tal que $\varpi_0=0$. Por lo tanto, ϱ es un caracter generador izquierdo por definición. □

1.9 Proposición. *Sea A un R-módulo izquierdo finito. Entonces A tiene un caracter generador izquierdo si y sólo si A puede incrustarse en $\widehat{R}$.*

Demostración. Si A está inserta en $\widehat{R}$, entonces A admite un caracter generador, por los Lemas 1.7 y 1.8.

A la inversa, sea ϱ un caracter generador de A. Para definir $f:A\to\widehat{R}$, emplearemos a ϱ de la siguiente forma. Para $a\in A$, definiremos a $f(a)\in\widehat{R}$ como $f(a)(r)=\varrho(ra)$, $r\in R$. Es sencillo verificar que f es un homomorfismo de R-módulo izquierdo de A a $\widehat{R}$. Si $a\in\ker f$, entonces $\varrho(ra)=0$ para toda $r\in R$. Así, el R-submódulo izquierdo $Ra\subset\ker\varrho$. Puesto que ϱ es un caracter generador, se concluye que $Ra=0$. Por lo tanto, $a=0$, y f es inyectiva. □

Cuando $A=R$, la Proposición 1.9 es consistente con la definición de caracter generador de un anillo. De hecho, si R está inserto en $\widehat{R}$, entonces R y $\widehat{R}$ son isomorfos como módulos de un sólo lado, pues tienen el mismo número de elementos.

1.10 Teorema. *Sea $R = M_m(\mathbb{F}_q)$ el anillo de matrices de $m \times m$ sobre un campo finito $\mathbb{F}_q$. Sea $A = M_{m\times k}(\mathbb{F}_q)$ el R-módulo izquierdo de todas las matrices de $m \times k$ sobre $\mathbb{F}_q$. Entonces A admite un caracter generador izquierdo si y sólo si $m \geq k$.*

Demostración. Si $m \geq k$, entonces, añadiendo $m - k$ columnas de ceros, A puede insertarse dentro de R como ideal izquierdo. Por el Ejemplo 1.3 y el Lema 1.7, A admite un caracter generador. A la inversa, supongamos que $m < k$. Se probará que ningún caracter de A es un caracter generador de A. Para ello, sea ϖ cualquier caracter de A. Por el Ejemplo, 1.3, ϖ tiene la forma ϖ_Q para alguna matriz Q de $k \times m$ sobre $\mathbb{F}_q$. Dado que $k > m$, los renglones de Q son linealmente dependientes sobre $\mathbb{F}_q$. Sea P cualquier matriz distinta de cero sobre $\mathbb{F}_q$ de tamaño $m \times k$ tal que $PQ = 0$. Tal matriz P existe porque los renglones de Q son linealmente dependientes: pueden usarse los coeficientes de una relación de dependencia distinta de cero como las entradas de un renglón de P. Afirmamos que el submódulo izquierdo distinto de cero de A generado por P está contenido en el ker ϖ_Q. En efecto, para cualquier $B \in R$,

$$\varpi_Q(BP) = \upsilon_q(\mathrm{tr}(Q(BP))) = \upsilon_q(\mathrm{tr}((BP)Q)) = \upsilon_q(\mathrm{tr}(B(PQ))) = 0,$$

empleando el hecho de que $PQ = 0$ y la propiedad de que $\mathrm{tr}(BC) = \mathrm{tr}(CB)$. Por lo tanto, ningún caracter de A es un caracter generador. □

1.11 Proposición. *Supongamos que A es un R-módulo izquierdo finito. Entonces A admite un caracter generador izquierdo si y sólo si* $\mathrm{soc}(A)$ *admite un caracter generador izquierdo.*

Demostración. Si A admite un caracter generador, entonces también el $\mathrm{soc}(A)$, por el Lema 1.7.

A la inversa, supongamos que $\mathrm{soc}(A)$ admite un caracter generador υ. Por medio de la secuencia corta (1.4), sea ϱ cualquier extensión de υ a un caracter de A. Afirmamos que ϱ es un caracter generador de A. Para ello, supondremos que B es un submódulo de A tal que $B \subset \ker \varrho$. Entonces, $\mathrm{soc}(B) \subset \mathrm{soc}(A) \cap \ker \varrho = \mathrm{soc}(A) \cap \ker \upsilon$, ya que ϱ es una extensión de υ. Pero υ es un caracter generador de $\mathrm{soc}(A)$, por lo que $\mathrm{soc}(B) = 0$. Dado que B es un módulo finito, puede concluirse que $B = 0$. En consecuencia, ϱ es un caracter generador de A. □

1.12 Corolario. *Sea A un R-módulo izquierdo finito. Supongamos que* $\mathrm{soc}(A)$ *admite un caracter generador izquierdo υ. Entonces, cualquier extensión de υ a un caracter de A es un caracter generador izquierdo de A.*

Finalmente se probara el teorema que caracteriza a los anillos de Frobenius finitos a través de sus caracteres.

1.13 Teorema. *Sea R un anillo finito. Entonces, las afirmaciones siguientes son equivalentes:*

i) *R es de Frobenius;*

ii) *R tiene un caracter generador izquierdo, es decir, $\widehat{R}$ es un R-módulo izquierdo libre;*

iii) *R tiene un caracter generador derecho, es decir, $\widehat{R}$ es un R-módulo derecho libre.*

Además, cuando estas condiciones se satisfacen, todo caracter generador izquierdo es también un caracter generador derecho y viceversa.

Demostración. Las afirmaciones *ii*) y *iii*) son equivalentes por la Proposición 1.5. Ahora se demostrará que *iii*) implica *i*).

Por el Ejemplo 1.3, el R-módulo $(R/\mathrm{rad}\,(R))_R$ es igual al módulo caracter del R-módulo izquierdo ${}_R\,(R/\mathrm{rad}\,(R))$. Por la Proposición 1.6 aplicada al R-módulo izquierdo

$$A = {}_RR,$$

tenemos que ${}_R\,(R/\mathrm{rad}\,(R))\widehat{\ } \cong \mathrm{soc}\left(\widehat{R}_R\right) \cong \mathrm{soc}\,(R_R)$, ya que se asume que $\widehat{R}$ es derecho y libre. De este modo, se tiene el isomorfismo $(R/\mathrm{rad}\,(R))_R \cong \mathrm{soc}\,(R_R)$ de R-módulos derechos. Puede repetirse este argumento para un isomorfismo por la izquierda (empleando *ii*)).

Ahora, asumamos que se verifica *i*). Gracias a (1.1), se observa que el que R sea de Frobenius implica que $\mathrm{soc}\,(R)$ es la suma de módulos de matrices de la forma $M_{m_i}(\mathbb{F}_{q_i})$. Por el Teorema 1.10 y sumando, $\mathrm{soc}\,(R)$ admite un caracter generador izquierdo. Por las proposiciones 1.4 y 1.11, R admite él mismo un caracter generador izquierdo. Por lo tanto, *ii*) se verifica. □

Para terminar esta sección puntualizaremos las similitudes entre una álgebra de Frobenius general (no necesariamente finita) y un anillo de Frobenius finito.

1.14 Definición. Una álgebra de dimensión finita A sobre un campo F es una *álgebra de Frobenius* si existe una función lineal: $\lambda : A \to F$ tal que $\ker \lambda$ no contiene ideales izquierdos distintos de cero.

Aparentemente, la estructura funcional de λ juega un papel en una álgebra de Frobenius comparable al del caracter generador izquierdo ϱ de un anillo finito de Frobenius. Como podría esperarse, la conexión entre λ y ϱ es aún más fuerte cuando se considera a una álgebra de Frobenius finita. Recordemos, por el Ejemplo 1.2, que todo campo finito $\mathbb{F}_q$ admite un caracter generador υ_q.

1.15 Teorema. *Sea R una álgebra de Frobenius sobre un campo finito $\mathbb{F}_q$, con estructura funcional $\lambda : R \to \mathbb{F}_q$. Entonces R es una anillo de Frobenius finito con caracter generador izquierdo $\varrho = \upsilon_q \circ \lambda$.*

A la inversa, supongamos que R es una álgebra de dimensión finita sobre un campo finito $\mathbb{F}_q$ y que R es un anillo de Frobenius con caracter generador ϱ. Entonces R es una álgebra de Frobenius, y existe una estructura funcional $\lambda : R \to \mathbb{F}_q$ tal que $\varrho = \upsilon_q \circ \lambda$.

Demostración. Tanto $R^* := \mathrm{Hom}_{\mathbb{F}_q}(R, \mathbb{F}_q)$ y $\widehat{R} = \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})$ son (R,R)-bimódulos que satisfacen $|R^*| = \left|\widehat{R}\right| = |R|$. Un caracter generador υ_q de $\mathbb{F}_q$ induce un homomorfismo de bimódulos $f : R^* \to \widehat{R}$ por medio de $\lambda \mapsto \upsilon_q \circ \lambda$. Pretendemos que f sea inyectiva. Para ello, supongamos que $\lambda \in \ker f$. Entonces $\upsilon_q \circ \lambda = 0$, de manera que $\lambda(R) \subset \ker \upsilon_q$. Notemos que $\lambda(R)$ es un subespacio vectorial sobre $\mathbb{F}_q$ contenido en $\ker \upsilon_q \subset \mathbb{F}_q$. Debido a que υ_q es un caracter generador de $\mathbb{F}_q$, por la Proposición 1.4, $\lambda(R) = 0$. Por lo tanto, $\lambda = 0$, y f es inyectiva. Como $|R^*| = \left|\widehat{R}\right|$, f es de hecho un isomorfismo de bimódulo.

Haremos que la estructura funcional en R^* corresponda bajo f a los caracteres generadores en $\widehat{R}$. Esto es, si $\varpi = f(\lambda)$, donde $\lambda \in R^*$ y $\varpi \in \widehat{R}$, entonces λ satisface la condición de que el $\ker \lambda$ no contiene ideales izquierdos distintos de cero de R si y sólo si ϖ es un caracter generador de R, es decir, $\ker \varpi$ no contiene ideales izquierdos distintos de cero de R.

Supongamos que ϖ es un caracter generador de R, y que I es un ideal izquierdo de R con $I \subset \ker \lambda$. Puesto que $\varpi = \upsilon_q \circ \lambda$, también tenemos que $I \subset \ker \varpi$. Dado que ϖ es un caracter generador, la Proposición 1.4 implica que $I = 0$, como se deseaba.

A la inversa, supongamos que λ satisface la condición de que $\ker \lambda$ no contiene ideales izquierdos distintos de cero de R, y supongamos que I es un ideal izquierdo de R con $I \subset \ker \varpi$. Entonces $\lambda(I)$ es un subespacio lineal sobre $\mathbb{F}_q$ dentro de $\ker \upsilon_q \subset \mathbb{F}_q$. Dado que υ_q es un caracter generador de $\mathbb{F}_q$, se sigue que $\lambda(I) = 0$, es decir, $I \subset \ker \lambda$. Por la condición en λ, se concluye que $I = 0$, como se requería. □

1.2. Teoría de Códigos

Los códigos correctores de errores proven una forma de proteger mensajes de corrupciones producidas durante su transmisión o almacenamiento. Esto se logra al añadir redundancia a la información de forma tal que, con una alta probabilidad, el mensaje original pueda recuperarse a partir del mensaje recibido.

Sea I el conjunto finito de información con los posibles mensajes que pueden ser enviados o transmitidos. Sea A otro conjunto finito con el *alfabeto* con el que se pretende hacer la codificación. La *codificación* del conjunto de información es la función inyectiva

$$f : I \to A^n$$

para alguna n y la imagen $f(I)$ es un código en A^n. Por ejemplo, un pixel de una imagen digital almacena la información de su tono o luminosidad en formato binario. En una imagen digital en escala de grises, cada pixel se almacena en un Byte, donde su valor numérico representa su tono, que puede oscilar entre el blanco (255) y el negro (0). Esto quiere decir que es una imagen en donde existen 256 tonos de gris (de 0 a 255, ambos inclusive). El conjunto I es el de los posibles tonos de la imagen; el alfabeto, $A = \{0, 1\}$ (binario); y la codificación, aquella que asigna a cada uno de los 256 tonos una secuencia binaria específica de 8 bits.

Para un mensaje dado $x \in I$, la cadena $f(x)$ se transmite por medio de un canal (un cable de cobre, fibra óptica, el almacenamiento mediante dispositivos digitales, la transmisión por radio o teléfono celular, por ejemplo). Durante este proceso de transmisión, algunas de las entradas en la cadena $f(x)$ puede alterarse, de forma tal que la cadena $y \in A^n$ recibida puede ser distinta a la cadena $f(x)$ enviada originalmente.

El objetivo de la Teoría de Códigos es elegir, para un canal dado, una codificación f en forma tal que sea posible, con una alta probabilidad, recuperar el mensaje original x con sólo conocer el mensaje recibido y y el método empleado para hacer la codificación. Al proceso de recuperar al mensaje original x se le llama *decodificación*.

Fue un teorema de Claude Shannon [62], en 1948, que lanzó a la Teoría de Códigos a un camino de investigación permanente. En éste se señala que, hasta cierto límite determinado por el canal, siempre es posible encontrar una codificación que será decodificada con tan alta probabilidad como sea deseada mientras la longitud n de la codificación sea lo suficientemente larga. La demostración de Shannon no es constructiva; tampoco brinda un método de codificación ni describe cómo hacer la decodificación. Gran parte de la investigación sobre Teoría de Códigos desde la publicación de aquel teorema ha

estado enfocada, precisamente, a hallar códigos eficientes y a desarrollar algoritmos de decodificación eficaces ([29] y [52] son referencias obligadas sobre el tema).

Ahora bien, se poseen más herramientas para construir códigos si se asume que el alfabeto A y los códigos $C \subset A^n$ están provistos de una estructura algebraica. El primer caso, el de la teoría clásica, es aquel en el que se asume que A es un campo finito y que $C \subset A^n$ es un subespacio lineal.

1.16 Definición. Sea $\mathbb{F}$ un campo finito. Un *código lineal* de longitud n sobre $\mathbb{F}$ es un subespacio lineal $C \subset \mathbb{F}^n$. La dimensión del código lineal se denota por $k = \dim_{\mathbb{F}} C$.

Dados dos vectores $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in \mathbb{F}^n$, su *distancia de Hamming* $d(x, y) = |\{i : x_i \neq y_i\}|$ es el número de posiciones en las que los vectores difieren. El *peso de Hamming* $\mathrm{wt}(x) = d(x, 0)$ de un vector $x \in \mathbb{F}^n$ es el número de posiciones en las que el vector es distinto de cero. Notemos que $d(x, y) = \mathrm{wt}(x - y)$; d es simétrica y satisface la desigualdad del triángulo. La *distancia mínima* de un código $C \subset \mathbb{F}^n$ es el valor más pequeño d_C de $d(x, y)$ para $x \neq y$, $x, y \in C$. Cuando C es un código lineal, d_C es igual al menor valor de $\mathrm{wt}(x)$ para $x \neq 0$, $x \in C$.

La distancia mínima de un código C es una medida asociada a la capacidad del código para corregir errores. Sea $B(x, r) = \{y \in \mathbb{F}^n : d(x, y) \leq r\}$ la bola en $\mathbb{F}^n$ con centro en x y radio r. Sea $r_0 = [(d_C - 1)/2]$, el mayor entero menor o igual a $(d_C - 1)/2$. Entonces, todas las bolas $B(x, r_0)$ para $x \in C$ son disjuntas. Supongamos que se transmite $x \in C$, que se recibe $y \in \mathbb{F}^n$ y que decodificamos a y como el elemento más cercano en el código C (y desempatamos al azar en caso de empate). Si a lo más r_0 entradas de x son distorsionadas durante la transmisión, entonces este método siempre produce una decodificación correcta. Se dice que C corrige entonces r_0 errores. Mientras mayor sea d_C, mayor será el número de errores que pueden corregirse. Es útil pues seguir la pista de los pesos de todos los elementos de un código C.

1.17 Definición. El *enumerador del peso de Hamming* $W_C(X, Y)$ es el polinomio (función generadora) definido por

$$W_C(X, Y) = \sum_{x \in C} X^{n - \mathrm{wt}(x)} Y^{\mathrm{wt}(x)} = \sum_{i=0}^{n} A_i X^{n-i} Y^i,$$

donde A_i es el número de elementos del peso i en C.

Sólo el vector cero tiene peso 0. En un código lineal, $A_0 = 1$ y $A_i = 0$ para $0 < i < d_C$.

Definamos un producto interno en $\mathbb{F}^n$ por

$$x \cdot y = \sum_{i=1}^{n} x_i y_i, \quad x = (x_1, \ldots, x_n), \quad y = (y_1, \ldots, y_n) \in \mathbb{F}^n.$$

Asociado a cada código lineal $C \subset \mathbb{F}^n$ está su *código dual* $C^\perp$:

$$C^\perp = \{y \in \mathbb{F}^n : \ x \cdot y = 0, x \in C\}.$$

Si $k = \dim C$, entonces $\dim C^\perp = n - k$.

Uno de los resultados más famosos en la Teoría de Códigos relaciona el enumerador del peso de Hamming de un código lineal C con su código dual $C^\perp$: las identidades de MacWilliams, las cuales se estudiarán a mayor profundidad en la siguiente sección. Por el momento, sólo se enunciarán.

1.18 Teorema (Las identidades de MacWilliams)**.** *Sea C un código lineal en $\mathbb{F}_q^n$. Entonces*

$$W_C(X, Y) = \frac{1}{|C^\perp|} W_{C^\perp}(X + (q-1)Y, X - Y).$$

De especial interés son los códigos autoduales. Un código lineal C es *auto ortogonal* si $C \subset C^\perp$; C es *auto dual* si $C = C^\perp$. Un código auto dual C de longitud n y dimensión k satisface $n = 2k$, de manera que n debe ser par.

Aunque hay trabajos recientes sobre códigos lineales definidos sobre los anillos $\mathbb{Z}/k\mathbb{Z}$, en 1994, el artículo de Hammons y otros [23] marcó un hito. En dicho artículo se explicaba el fenómeno de dos familias de códigos lineales binarios que parecían duales; sus enumeradores del peso de Hamming satisfacían las identidades de MacWilliams. Los autores descubrieron que dos familias de código lineales sobre $\mathbb{Z}/4\mathbb{Z}$ que eran duales entre sí y, por lo tanto, sus enumeradores satisfacían las identidades de MacWilliams. Adicionalmente, por medio del mapeo de Gray $g : \mathbb{Z}/4\mathbb{Z} \to \mathbb{F}_2^2$ definido por $g(0) = 00$, $g(1) = 01$, $g(2) = 11$ y $g(3) = 10$ (g no es un homomorfismo), los autores mostraron que las dos familias de códigos lineales sobre $\mathbb{Z}/4\mathbb{Z}$ eran mapeadas a las familias originales de códigos no lineales sobre $\mathbb{F}_2$. A partir de entonces se despertó el interés por estudiar códigos lineales definidos sobre anillos, el cual continúa al día de hoy.

1.19 Definición. Sea R un anillo finito. Un *código lineal izquierdo* C de longitud n sobre R es un R-submódulo izquierdo $C \subset R^n$.

La definición de código lineal derecho es análoga.

1.20 Definición. Sea R un anillo finito, y sea A (el *alfabeto*) un R-módulo finito izquierdo. Un código lineal izquierdo C de longitud n sobre A es un R-submódulo izquierdo $C \subset A^n$.

El peso de Hamming se define en la misma forma que en el caso de los campos finitos. Para $x = (x_1, x_2, \ldots, x_n) \in R^n$ (o A^n), se define como $\mathrm{wt}(x) = |\{i : x_i \neq 0\}|$, el número de entradas distintas de cero en el vector x.

1.3. Las identidades de MacWilliams

En esta sección se presenta una demostración de las identidades de MacWilliams que es válida para cualquier anillo de Frobenius finito. La prueba, que corresponde a la publicada en [**?**, Teorema 8.3] es esencialmente la misma atribuida a Gleason en [2, §1.12]. Las identidades de MacWilliams se cumplen aun en escenarios más generales, pero el caso de los códigos lineales sobre un anillo de Frobenius finito destaca el papel que juegan los caracteres en la demostración.

Sea R un anillo finito. Como se hizo previamente para campos, definiremos un *producto punto* en R^n como

$$x\cdot = \sum_{i=1}^{n} x_i y_i, \quad x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in R^n.$$

Para un código lineal izquierdo $C \subset R^n$, definamos el *aniquilador derecho* $r(C)$ como $r(C) = \{y \in R^n : x \cdot y = 0, x \in C\}$. El aniquilador derecho jugará el papel del código dual $C^{\perp}$. Dado que R puede ser no conmutativo, se debe elegir ya sea el aniquilador izquierdo o el derecho. El enumerador del peso de Hamming $W_C(X, Y)$ de un código lineal izquierdo C se define exactamente igual como en los campos.

1.21 Teorema (Las identidades de MacWilliams)**.** *Sea R un anillo de Frobenius finito, y sea $C \subset R^n$ un código lineal izquierdo. Entonces,*

$$W_C(X, Y) = \frac{1}{|r(C)|} W_{r(C)}(X + (|R| - 1)Y, X - Y).$$

La demostración de Gleason de las identidades de MacWilliams hace uso de la transformada de Fourier y de la fórmula de Poisson para la suma, mismos que se describen a continuación. Sea $(G, +)$ un grupo abeliano finito.

A lo largo de esta sección, se empleará la forma multiplicativa de caracteres; esto es, los caracteres son homomorfismos de grupo $\pi : (G, +) \to (\mathbb{C}^\times, \cdot)$ de un grupo abeliano finito a un grupo multiplicativo de números complejos distintos de cero. El conjunto $\widehat{G}$ de todos los caracteres de G forma un grupo abeliano bajo la multiplicación elemento a elemento. Las siguientes propiedades de los caracteres son bien conocidas y se presentan sin demostración. Se sugieren [61] y [73] para su revisión detallada.

1.22 Lema. *Para $x \in G$ y $\pi \in \widehat{G}$, los caracteres de un grupo abeliano finito G tienen las siguientes propiedades:*

i) $\left|\widehat{G}\right| = |G|$;

ii) $(G_1 \times G_2) \cong \widehat{G}_1 \times \widehat{G}_2$;

iii) $\sum_{x \in G} \pi(x) = \begin{cases} |G|, & \pi = 1 \\ 0, & \pi \neq 1; \end{cases}$

iv) $\sum_{\pi \in \widehat{G}} \pi(x) = \begin{cases} |G|, & x = 0, \\ 0, & x \neq 0; \end{cases}$

v) *Los caracteres forman un subconjunto linealmente independiente del espacio vectorial de funciones valuadas en los complejos de G. De hecho, los caracteres forman una base.*

Sea V un espacio vectorial sobre los números complejos. Para cualquier función

$$f : G \to V,$$

definamos su *transformada de Fourier* $\widehat{f} : \widehat{G} \to V$ como

$$\widehat{f}(\pi) = \sum_{x \in G} \pi(x) f(x), \quad \pi \in \widehat{G}.$$

Dado un subgrupo $H \subset G$, definamos su *aniquilador* $\left(\widehat{G} : H\right) = \left\{\pi \in \widehat{G} : \pi(H) = 1\right\}$. Como se mostró en (1.5), $\left|\left(\widehat{G} : H\right)\right| = |G| / |H|$.

1.23 Proposición (Fórmula de Poisson para la suma)**.** *Sea $H \subset G$ un subgrupo, y sea $f : G \to V$ cualquier función de G a un espacio vectorial V sobre los complejos. Entonces*

$$\sum_{x \in H} f(x) = \frac{1}{\left|\left(\widehat{G} : H\right)\right|} \sum_{\pi \in \left(\widehat{G} : H\right)} \widehat{f}(\pi).$$

El siguiente resultado describe la transformada de Fourier de una función, que es el producto de funciones de una variable.

1.24 Lema. *Supongamos que V es una álgebra conmutativa sobre los números complejos, y supongamos que $f_i : G \to V$, $i = 1, \ldots, n$, son funciones de G a V. Sea $f : G^n \to V$ definida como $f(x_1, \ldots, x_n) = \prod_{i=1}^n f_i(x_i)$. Entonces,*

$$\widehat{f}(\pi_1, \ldots, \pi_n) = \prod_{i=1}^n \widehat{f_i}(\pi_i).$$

Demostración del Teorema 1.21. Dado un código lineal izquierdo $C \subset R^n$, apliquemos la fórmula de Poisson para la suma con $G = R^n$, $H = C$ y $V = \mathbb{C}[X, Y]$, el anillo polinomial sobre $\mathbb{C}$ en dos indeterminados. Definamos $f_i : R \to \mathbb{C}[X, Y]$ como

$$f_i(x_i) = X^{1-\mathrm{wt}(x_i)} Y^{\mathrm{wt}(x_i)},$$

$x_i \in R$, donde $\mathrm{wt}(r) = 0$ para $r = 0$, y $\mathrm{wt}(r) = 1$ para $r \neq 0$ en R. Sea $f : R^n \to \mathbb{C}[X, Y]$ el producto de las f_i; es decir,

$$f(x_1, \ldots, x_n) = \prod_{i=1}^n X^{1-\mathrm{wt}(x_i)} Y^{\mathrm{wt}(x_i)} = X^{n-\mathrm{wt}(x)} Y^{\mathrm{wt}(x)},$$

donde $x = (x_1, \ldots, x_n) \in R^n$. Es claro que $\sum_{x \in H} f(x)$, el lado izquierdo de la fórmula de Poisson para la suma, es simplemente el enumerador del peso de Hamming $W_C(X, Y)$.

Para simplificar el lado derecho de la fórmula de Poisson para la suma, debemos calcular $\widehat{f}$. Por el Lema 1.24, primero se calculará $\widehat{f_i}$.

$$\begin{aligned}
\widehat{f_i}(\pi_i) &= \sum_{a \in R} \pi_i(a) f_i(a) \\
&= \sum_{a \in R} \pi_i(a) X^{1-\mathrm{wt}(a)} Y^{\mathrm{wt}(a)} \\
&= X + \sum_{a \neq 0} \pi_i(a) Y \\
&= \begin{cases} X + (|R| - 1) Y, & \pi_i = 1, \\ X - Y, & \pi_i \neq 1. \end{cases}
\end{aligned}$$

En la penúltima línea, se evalúa el caso $a = 0$ contra todos los casos en los que $a \neq 0$. Para llegar a la última línea, se hace uso del Lema 1.22. Con el Lema 1.24 se tiene que

$$\widehat{f}(\pi) = (X + (|R| - 1)Y)^{n-\mathrm{wt}(\pi)} (X - Y)^{\mathrm{wt}(\pi)},$$

donde $\pi = (\pi_1, \ldots, \pi_n) \in \widehat{R}^n$ y $\mathrm{wt}(\pi)$ cuenta el número de π_i tales que $\pi_i \neq 1$.

Resta identificar el caracter aniquilador $\left(\widehat{G} : H\right) = \left(\widehat{R}^n : C\right)$ con $r(C)$, que es en donde los anillos de Frobenius entran en escena. Sea ρ un caracter generador de R. Emplearemos ρ para definir un homomorfismo $\beta : R \to \widehat{R}$. Para $r \in R$, el caracter $\beta(r) \in \widehat{R}$ tiene la forma $\beta(r)(s) = (r\rho)(s)$ para $s \in R$. Es posible verificar que

$$\beta : R \to \widehat{R}$$

es un isomorfismo de R-módulos izquierdos. En particular, $\mathrm{wt}(r) = \mathrm{wt}(\beta(r))$.

Extendamos β a un isomorfismo $\beta : R^n \to \widehat{R}^n$ de R-módulos izquierdos, por medio de $\beta(x)(y) = \rho(y \cdot x)$, para $x, y \in R^n$. De nuevo, $\mathrm{wt}(x) = \mathrm{wt}(\beta(x))$. Para $x \in R^n$, $\beta(x) \in \left(\widehat{R}^n : C\right)$ ocurre cuando $\beta(x)(C) = 1$, esto es, cuando $\rho(C \cdot x) = 1$. Esto significa que el ideal izquierdo $C \cdot x$ de R está contenido en el ker ρ. Puesto que ρ es un caracter generador, la Proposición 1.4 implica que $C \cdot x = 0$. Así, $x \in r(C)$. El resultado a la inversa es claro. Por lo tanto, $r(C)$ corresponde a $\left(\widehat{R}^n : C\right)$ bajo el isomorfismo β.

El lado derecho de la fórmula de Poisson para la suma ahora puede simplificarse como sigue:

$$\begin{aligned}\frac{1}{\left|\left(\widehat{G} : H\right)\right|} \sum_{\pi \in \left(\widehat{G}:H\right)} \widehat{f}(\pi) &= \frac{1}{|r(C)|} \sum_{x \in r(C)} (X + (|R| - 1)Y)^{n-\mathrm{wt}(x)} (X - Y)^{\mathrm{wt}(x)} \\ &= \frac{1}{|r(C)|} W_{r(C)}(X + (|R| - 1)Y, X - Y),\end{aligned}$$

como se deseaba. □

1.4. La Extensión del teorema de MacWilliams

Para concluir con el capítulo se presentará el problema de la extensión, mismo que se originó al estudiar la equivalencia entre códigos. El resultado principal es que un

anillo finito tiene la propiedad de la extensión para códigos lineales respecto al peso de Hamming si y sólo si el anillo es de Frobenius.

Dos códigos lineales deben considerarse equivalentes bajo dos enfoques: por medio de transformaciones monomiales o bien a través de isomorfismos que preserven el peso.

1.25 Definición. Sea R un anillo finito. Una *transformación monomial* izquierda $T : R^n \to R^n$ es un homomorfismo lineal izquierdo sobre R de la forma

$$T(x_1, \ldots, x_n) = \left(x_{\sigma(1)}u_1, \ldots, x_{\sigma(n)}u_n\right), \quad (x_1, \ldots, x_n) \in R^n,$$

para alguna permutación σ de $\{1, 2, \ldots, n\}$ y unidades $u_1, \ldots, u_n$ de R.

Dos códigos lineales izquierdos $C_1, C_2 \subset R^n$ son *equivalentes* si existe una transformación monomial $T : R^n \to R^n$ tal que $T(C_1) = C_2$.

Otra forma de definir a dos códigos equivalentes $C_1, C_2 \subset R^n$ es la siguiente: si existe un isomorfismo lineal sobre R, $f : C_1 \to C_2$, que preserve el peso de Hamming - es decir, tal que $\mathrm{wt}(f(x)) = \mathrm{wt}(x)$, para toda $x \in C_1$- entonces los códigos son equivalentes. El siguiente lema muestra que el concepto de equivalencia mediante transformaciones monomiales implica la equivalencia empleando isomorfismos que preserven el peso de Hamming.

1.26 Lema. *Si $T : R^n \to R^n$ es una transformación monomial, entonces T preserva el peso de Hamming $\mathrm{wt}(T(x)) = \mathrm{wt}(x)$, para toda $x \in R^n$. Si dos códigos lineales $C_1, C_2 \subset R^n$ son equivalentes por medio de la transformación monomial T, entonces la restricción f de T a C_1 es un isomorfismo lineal sobre R, $C_1 \to C_2$, que preserva el peso de Hamming.*

Demostración. Para cualquier $r \in R$ y cualquier unidad $u \in R$, $r = 0$ si y sólo si $ru = 0$, hecho del cual se sigue el resultado. □

Cabe preguntarse si el resultado se cumple a la inversa, es decir, si dados $C_1, C_2 \in R^n$ y un isomorfismo lineal sobre R, $f : C_1 \to C_2$, que preserve el peso de Hamming, f se extiende a una transformación monomial $T : R^n \to R^n$. Este es, justamente, el problema de la extensión, mismo que se estudiará en términos de una propiedad.

1.27 Definición. Sea R un anillo finito. El anillo R tiene la *propiedad de la extensión* (PE) con respecto al peso de Hamming si siempre que dos códigos lineales izquierdos $C_1, C_2 \subset R^n$ admitan un isomorfismo lineal sobre R, $f : C_1 \to C_2$, que preserve el peso de Hamming se sigue que f se extiende a una transformación monomial $T : R^n \to R^n$.

De manera que, las dos nociones de equivalencia coinciden precisamente cuando el anillo R satisface la propiedad de extensión. MacWilliams halló que los campos finitos tienen esta propiedad (véanse [50] y [51]). Otros investigadores, como Bogart, Goldberg y Gordon [6] o Ward y Wood [74] han brindado demostraciones alternativas que prueban este hecho. No se revisará este caso por ser un caso particular del teorema principal de esta sección.

1.28 Teorema. *Sea R un anillo finito. Entonces R tiene la propiedad de la extensión con respecto al peso de Hamming si y sólo si R es de Frobenius.*

El hecho de que los anillos de Frobenius tienen esta propiedad, apareció por primera vez en [**?**, Teorema 6.3]. La demostración, que se presentará en breve, está basada en la independencia lineal de caracteres y se aborda para el caso de los campos finitos en [74]. Otra prueba, bajo un enfoque combinatorio, lo presentan Greferath y Schimidt en [22]. De forma más general, Greferath, Nechaev y Wisbauer mostraron que el módulo caracter de cualquier anillo finito tiene la propiedad de extensión para los pesos de Hamming y los pesos homogéneos [21].

El hecho en la dirección inversa, que sólo los anillos finitos de Frobenius tienen la propiedad de la extensión, apareció por primera vez en [78], artículo en el que se tomó una estrategia propuesta por [17].

A continuación se abordarán los resultados necesarios para probar este importante teorema. Comenzaremos pues probando que todo anillo de Frobenius finito tiene la propiedad de extensión, siguiendo el tratamiento dado en [**?**, Teorema 6.3].

Asumamos que $C_1, C_2 \subset R^n$ son dos códigos lineales izquierdos y que $f : C_1 \to C_2$ es un isomorfismo lineal sobre R que preserva el peso de Hamming. Debe probarse que f se extiende a una transformación monomial de R^n. La idea principal es expresar la propiedad de la preservación del peso de f como una ecuación de caracteres de C_1 y usar la independencia lineal de los caracteres para empatar términos.

Sean $\mathrm{pr}_1, \ldots, \mathrm{pr}_n : R^n \to R$ las proyecciones de las coordenadas, de manera que $\mathrm{pr}_i(x_1, \ldots, x_n) = x_i$, $(x_1, \ldots, x_n) \in R^n$. Denotemos con $\lambda_1, \ldots, \lambda_n$ las restricciones de $\mathrm{pr}_1, \ldots, \mathrm{pr}_n$ a $C_1 \subset R^n$. De forma similar, sean $\mu_1, \ldots, \mu_n : C_1 \to R$ dadas por $\mu_i = \mathrm{pr}_i \circ f$. Entonces, $\lambda_1, \ldots, \lambda_n$, $\mu_1, \ldots, \mu_n \in \mathrm{Hom}_R(C_1, R)$ son funciones lineales izquierdas sobre R en C_1. Bastará con demostrar la existencia de una permutación σ de $\{1, \ldots, n\}$ y de unidades $u_1, \ldots, u_n$ de R tales que $\mu_i = \lambda_{\sigma(i)} u_i$, para $i = 1, \ldots, n$.

Para cualquier $x \in C_1$, el peso de Hamming de x está dado por $\mathrm{wt}(x) = \sum_{i=1}^{n} \mathrm{wt}(\lambda_i(x))$,

mientras que el peso de Hamming de $f(x)$ está dado por $\mathrm{wt}(f(x)) = \sum_{i=1}^{n} \mathrm{wt}(\mu_i(x))$. Dado que f preserva el peso de Hamming, se tiene que

$$\sum_{i=1}^{n} \mathrm{wt}(\lambda_i(x)) = \sum_{i=1}^{n} \mathrm{wt}(\mu_i(x)). \tag{1.6}$$

Al emplear el Lema 1.22 se observa que

$$1 - \mathrm{wt}(r) = \frac{1}{|R|} \sum_{\pi \in \widehat{R}} \pi(r),$$

para cualquier $r \in R$. Al aplicar esto a (1.6) y simplificar, se sigue que

$$\sum_{i=1}^{n} \sum_{\pi \in \widehat{R}} \pi(\lambda_i(x)) = \sum_{i=1}^{n} \sum_{\pi \in \widehat{R}} \pi(\mu_i(x)), \quad x \in C_1. \tag{1.7}$$

Ya que se asume que R es de Frobenius, entonces R admite un caracter generador izquierdo ρ. Todo caracter $\pi \in \widehat{R}$ tiene por lo tanto la forma $\pi = a\rho$, para alguna $a \in R$. Recordemos que el producto por un escalar significa que $\pi(r) = (a\rho)(r) = \rho(ra)$, para $r \in R$. Usando esto para simplificar (1.7) y diferentes subíndices en cada lado de la ecuación resultante se obtiene

$$\sum_{i=1}^{n} \sum_{a \in R} \rho \circ (\lambda_i a) = \sum_{j=1}^{n} \sum_{b \in R} \rho \circ (\mu_j b). \tag{1.8}$$

Esta es una ecuación de caracteres de C_1. Debido a que los caracteres son linealmente independientes, podemos empatar los términos de los miembros izquierdo y derecho de (1.8). Para obtener múltiplos de unidades, se debe tener especial cuidado.

Puesto que C_1 es un R-módulo izquierdo, $\mathrm{Hom}_R(C_1, R)$ es un R-módulo derecho. Definamos un preorden $\preceq$ en $\mathrm{Hom}_R(C_1, R)$ como $\lambda \preceq \mu$ si $\lambda = \mu r$ para alguna $r \in R$. Por un resultado de Bass [3, Lema 6.4], $\lambda \preceq \mu$ y $\mu \preceq \lambda$ implican que $\mu = \lambda u$ para alguna unidad u de R.

Entre las funciones lineales $\lambda_1, \ldots, \lambda_n$, $\mu_1, \ldots, \mu_n$ (una lista finita), puede elegirse una que sea maximal en el preorden $\preceq$. Sin pérdida de generalidad, asumamos que μ_1 es maximal en $\preceq$. Esto significa que si $\mu_1 \preceq \lambda$ para alguna λ, entonces $\mu_1 = \lambda u$ para alguna unidad u de R. En (1.8), consideremos el término del miembro derecho de la ecuación con $j = 1$ y $b = 1$. Por la independencia lineal de caracteres, existen i_1, $1 \leq i_1 \leq n$, y $a \in R$ tales que $\rho \circ (\lambda_{i_1} a) = \rho \circ \mu_1$. Esta ecuación implica que $\operatorname{im}(\mu_1 - \lambda_{i_1} a) \subset \ker \rho$. Pero $\operatorname{im}(\mu_1 - \lambda_{i_1} a)$ es un ideal izquierdo de R, y ρ es un caracter generador de R. Por la Proposición 1.4, $\operatorname{im}(\mu_1 - \lambda_{i_1} a) = 0$, por lo que $\mu_1 = \lambda_{i_1} a$. Esto quiere decir que $\mu_1 \preceq \lambda_{i_1}$. Como μ_1 se eligió como maximal, tenemos que $\mu_1 = \lambda_{i_1} u_1$ para alguna unidad u_1 de R. Comencemos a definir una permutación σ por $\sigma(1) = i_1$.

Al reindexar, todos los términos del lado izquierdo de (1.8) con $i = i_1$ coinciden los términos del lado derecho de (1.8) con $j = 1$. Esto es, $\sum_{a \in R} \rho \circ (\lambda_{i_1} a) = \sum_{b \in R} \rho \circ (\mu_1 a)$. Al sustraer esas sumas de (1.8) se reduce el tamaño de las sumas exteriores en uno. Por inducción, se obtiene el resultado deseado por medio de una permutación σ y hallando las unidades $u_1, \ldots, u_n$ de R.

Hasta este punto se ha probado que una condición suficiente para que un anillo satisfaga la propiedad de extensión con respecto al peso de Hamming es que éste sea de Frobenius. La prueba de este hecho se basa en la prueba del teorema de extensión sobre campos finitos que aprovecha la independencia lineal de los caracteres [74]. La prueba de que esta condición es además necesaria hace uso de la demostración del teorema de extensión de Bogart, et. al. [6], para lo cual se requiere reformular el problema de la extensión.

Todo código lineal izquierdo $C \subset R^n$ puede considerarse como la imagen del mapeo inclusión $C \to R^n$. De manera más general, todo código lineal izquierdo es la imagen de un homomorfismo lineal sobre R, $\Lambda : M \to R^n$, para algún R-módulo izquierdo finito M. Por medio de la composición con las proyecciones de coordenadas pr_i, el homomorfismo Λ puede expresarse como una n-tupla $\Lambda = (\lambda_1, \ldots, \lambda_n)$, donde cada $\lambda_i \in \operatorname{Hom}_R(M, R)$. Las λ_i se llaman *funcionales de las coordenadas* del código lineal.

Haremos un paréntesis para indicar que en la Teoría de Códigos es frecuente presentar un código lineal $C \subset R^n$ por medio de una *matriz generadora* G. La matriz G tiene entradas de R, el número de columnas de G es igual a la longitud n del código C, y -más importante aún- las filas de G generan a C como un submódulo izquierdo de R^n.

La descripción de un código lineal por medio de las funcionales de las coordenadas es equivalente esencialmente a aquella que emplea matrices generadoras. Si se tienen funcionales de coordenadas $\lambda_1, \ldots, \lambda_n$, puede producirse una matriz generadora G al elegir un conjunto $v_1, \ldots, v_k$ de generadores de C como módulo izquierdo sobre R y

tomando el valor de $\lambda_j(v_i)$ para las entradas (i,j) de G. A la inversa, dada una matriz generadora, sus columnas definen funcionales de coordenadas. Por lo tanto, el uso de funcionales de coordenadas constituye un enfoque de bases libres para las matrices generadoras. Esta idea aparece en [2].

Son de interés los códigos lineales equivalentes. Para un código lineal dado por

$$\Lambda = (\lambda_1, \ldots, \lambda_n) : M \to R^n,$$

el orden de las funcionales de coordenadas $\lambda_1, \ldots, \lambda_n$ es irrelevante, como lo es el reemplazo de cualquier λ_i por $\lambda_i u_i$, para alguna unidad u_i de R. La idea es codificar esta información de manera sistemática. Sea $\mathcal{U}$ el grupo de unidades del anillo R. El grupo $\mathcal{U}$ actúa sobre el módulo $\mathrm{Hom}_R(M,R)$ por medio de la multiplicación escalar derecha; sea $\mathcal{O}^\sharp$ el conjunto de órbitas de esta acción: $\mathcal{O}^\sharp = \mathrm{Hom}_R(M,R)/\mathcal{U}$. Entonces un código lineal $M \to R^n$, hasta la equivalencia, se especifica por medio de la elección de n elementos de $\mathcal{O}^\sharp$ (contando las multiplicidades). Esta elección puede ser codificada al especificar una función (una *función de multiplicidad*) $\eta : \mathcal{O}^\sharp \to \mathbb{N}$, los enteros no negativos, donde $\eta(\lambda)$ es el número de veces que λ (o una unidad múltiplo de λ) aparece como una funcional de coordenadas. La longitud n del código lineal está dada por $\sum_{\lambda \in \mathcal{O}^\sharp} \eta(\lambda)$.

En conclusión, los códigos lineales $M \to R^n$ (para M fija y cualquier n), hasta la equivalencia, están dadas por las funciones de multiplicidad $\eta : \mathcal{O}^\sharp \to \mathbb{N}$. Denotaremos el conjunto de todas esas funciones como $F\left(\mathcal{O}^\sharp, \mathbb{N}\right) = \left\{\eta : \mathcal{O}^\sharp \to \mathbb{N}\right\}$ y definiremos $F_0\left(\mathcal{O}^\sharp, \mathbb{N}\right) = \left\{\eta \in F\left(\mathcal{O}^\sharp, \mathbb{N}\right) : \eta(0) = 0\right\}$.

Es también de especial interés el peso de Hamming de las palabras código y cómo describir el peso de Hamming en términos de la función de multiplicidad Cη. Fijaremos una función de multiplicidad $\eta : \mathcal{O}^\sharp \to \mathbb{N}$. Definiremos $W_\eta : M \to \mathbb{N}$ como

$$W_\eta(x) = \sum_{\lambda \in \mathcal{O}^\sharp} \mathrm{wt}(\lambda(x))\,\eta(\lambda), \quad x \in M. \tag{1.9}$$

Entonces $W_\eta(x)$ es igual al peso de Hamming de la palabra código dada por $x \in M$. Cabe notar que $W_\eta(0) = 0$.

1.29 Lema. *Para $x \in M$ y una unidad $u \in \mathcal{U}$, $W_\eta(ux) = W_\eta(x)$.*

Demostración. El resultado se sigue de manera inmediata del hecho de que

$$\mathrm{wt}(ur) = \mathrm{wt}(r)$$

para $r \in R$ y una unidad $u \in \mathcal{U}$; esto es, $ur = 0$ si y sólo si $r = 0$. □

Dado que M es un R-módulo izquierdo, el grupo de unidades $\mathcal{U}$ actúa en M por la izquierda. Sea $\mathcal{O}$ el conjunto de órbitas de esta acción. Observemos que el Lema 1.29 implica que W_η es una función bien definida de $\mathcal{O}$ a $\mathbb{N}$. Sea $F(\mathcal{O}, \mathbb{N})$ el conjunto de todas las funciones de $\mathcal{O}$ a $\mathbb{N}$, y $F_0(\mathcal{O}, \mathbb{N}) = \{w \in F(\mathcal{O}, \mathbb{N})\}$ (recordemos que $W_\eta(0) = 0$). Por lo tanto, W asocia a todo código lineal, hasta la equivalencia, un listado de pesos de Hamming de todas las palabras código. Estos elementos, así como un argumento técnico del papel de las funcionales cero que se abordará en breve, prueba la siguiente reformulación de la propiedad de extensión.

1.30 Teorema. *Un anillo finito R tiene la propiedad de extensión con respecto al peso de Hamming si y sólo si la función*

$$W : F_0\left(\mathcal{O}^\sharp, \mathbb{N}\right) \to F_0(\mathcal{O}, \mathbb{N}), \quad \eta \mapsto W_\eta,$$

es inyectiva para todo R-módulo izquierdo finito M.

Observemos que los espacios de las funciones $F_0\left(\mathcal{O}^\sharp, \mathbb{N}\right)$, $F_0(\mathcal{O}, \mathbb{N})$ son monoides aditivos y

$$W : F_0\left(\mathcal{O}^\sharp, \mathbb{N}\right) \to F_0(\mathcal{O}, \mathbb{N})$$

es aditivo, es decir, un homomorfismo de monoides. Si se aplica el tensor con los números racionales $\mathbb{Q}$ (lo que significa que se permite que las funcionales de coordenadas tengan multiplicidades iguales a cualquier número racional), es posible generalizar el Teorema 1.30 a:

1.31 Teorema. *Un anillo finito R tiene la propiedad de extensión con respecto al peso de Hamming si y sólo si el homomorfismo lineal sobre $\mathbb{Q}$*

$$W : F_0\left(\mathcal{O}^\sharp, \mathbb{Q}\right) \to F_0(\mathcal{O}, \mathbb{Q}), \quad \eta \mapsto W_\eta,$$

es inyectivo para todo R-módulo izquierdo finito M.

El teorema anterior resulta conveniente debido a que los espacios de las funciones $F_0\left(\mathcal{O}^\sharp, \mathbb{Q}\right)$, $F_0(\mathcal{O}, \mathbb{Q})$ son espacios $\mathbb{Q}$-vectoriales y es posible emplear las herramientas del álgebra lineal sobre campos para analizar el homomorfismo lineal W. De hecho, en [6], Bogart y otros probaron el teorema de extensión sobre campos finitos al mostrar que la matriz que representa W es invertible. La forma de dicha matriz es aparente gracias a (1.9). Greferath generalizó dicho estudio en [20].

Para abordar el aspecto técnico pendiente se requiere una versión del Teorema 1.31 para códigos lineales definidos sobre un alfabeto A. Sea A un R-módulo izquierdo finito con el automorfismo de grupo $\mathrm{Aut}(A)$. Un código R-lineal izquierdo en A^n está dado por la imagen de un homomorfismo R-lineal $M \to A^n$, para algún R-módulo izquierdo

finito M. En este caso, las funcionales de coordenadas pertenecerán a $\mathrm{Hom}_R(M, A)$. El grupo $\mathrm{Aut}(A)$ actúa sobre $\mathrm{Hom}_R(M, A)$ por la derecha; sea $\mathcal{O}^\sharp$ el conjunto de órbitas de esta acción. Un código lineal sobre A, hasta la equivalencia, es especificado de nueva cuenta por la función de multiplicidad $\eta \in F\left(\mathcal{O}^\sharp, \mathbb{N}\right)$.

Como antes, el grupo de unidades $\mathcal{U}$ de R actúa en el módulo M por la izquierda, con el conjunto de órbitas $\mathcal{O}$. Se tiene entonces una formulación de la propiedad de extensión para el alfabeto A como:

1.32 Teorema. *Sea A un R-módulo izquierdo finito. Entonces A tiene la propiedad de extensión con respecto al peso de Hamming si y sólo si el homomorfismo lineal*

$$W : F_0\left(\mathcal{O}^\sharp, \mathbb{Q}\right) \to F_0\left(\mathcal{O}, \mathbb{Q}\right), \quad \eta \mapsto W_\eta,$$

es inyectivo para todo R-módulo izquierdo finito M.

Una vez reformulado el problema de la extensión, puede probarse que la condición necesaria para que un anillo satisfaga la propiedad de extensión con respecto al peso de Hamming es que éste sea de Frobenius. Se seguirá la estrategia planteada por Dinh y López Permouth [17], así como el Teorema 1.31 para probar la dirección contraria del Teorema 1.28, es decir, que si un anillo finito tiene la propiedad de extensión con respecto al peso de Hamming, entonces el anillo debe ser de Frobenius. Los pasos básicos de la estrategia son los siguientes:

i) Si el anillo finito R no es de Frobenius, entonces su soclo izquierdo contiene un R-módulo izquierdo de la forma $M_{m\times k}(\mathbb{F}_q)$ con $m < k$, para alguna q (compárense (1.1)y (1.3)).

ii) Usar la matriz módulo $M_{m\times k}(\mathbb{F}_q)$ como el alfabeto A. Si $m < k$, mostrar que A no tiene la propiedad de extensión.

iii) Tomar los contraejemplos de la propiedad de extensión sobre A. Considerarlos como R-módulos y mostrar que son también contraejemplos de la propiedad de extensión sobre R.

El primer y el último punto fueron probados en [17]. Una forma de ver el primer punto es la siguiente. Se sabe por (1.3) que el soclo $\mathrm{soc}({}_RR)$ es la suma de módulos de matrices $M_{m_i\times s_i}(\mathbb{F}_{q_i})$. Si $m_i \geq s_i$ para toda i, entonces cada una de las $M_{m_i\times s_i}(\mathbb{F}_{q_i})$ admitiría un caracter generador (por el Teorema 1.10). Al añadir esos caracteres generadores, se obtendrían caracteres generadores para $\mathrm{soc}({}_RR)$ mismo. Entonces, por la Proposición

1.11, R puede admitir un caracter generador y, en consecuencia, sería de Frobenius por el Teorema 1.13.

Para el tercer punto, consideremos los contraejemplos $C_1, C_2 \subset A^n$ a la propiedad de extensión para el alfabeto A respecto al peso de Hamming. Dado que

$$A^n \subset \operatorname{soc}({}_R R)^n \subset {}_R R^n,$$

C_1, C_2 pueden considerarse como R-módulos por medio de (1.1). El peso de Hamming para un elemento x de A^n es igual al peso de Hamming de x considerado como un elemento de R^n porque el peso de Hamming sólo depende de si las entradas de x son cero o no. De esta forma, C_1, C_2 también pueden ser contraejemplos a la propiedad de extensión para el alfabeto R con respecto al peso de Hamming.

De manera que el único punto pendiente de la estrategia es el segundo. Una construcción explícita de contraejemplos a la propiedad de extensión para el alfabeto $A = M_{n\times k}(\mathbb{F}_q)$, $m < k$ se propone en [78]. En dicho artículo se demuestra la existencia.

Sea $R = M_m(\mathbb{F}_q)$ el anillo de matrices de $m \times m$ sobre $\mathbb{F}_q$. Sea $A = M_{m\times k}(\mathbb{F}_q)$, con $m < k$. A es un R-módulo izquierdo. Por el Teorema 1.32, A no tendrá la propiedad de la extensión con respecto al peso de Hamming si se halla un R-módulo izquierdo finito M con $\dim_{\mathbb{Q}} F_0\left(\mathcal{O}^\sharp, \mathbb{Q}\right) > \dim_{\mathbb{Q}} F_0(\mathcal{O}, \mathbb{Q})$. Esta desigualdad se verificará para cualquier M distinta de cero.

Como R es simple, cualquier R-módulo izquierdo finito M tiene la forma $M = M_{m\times \ell}(\mathbb{F}_q)$, para alguna ℓ. Primero, se determina $\mathcal{O}$, que es el conjunto de todas las $\mathcal{U}$ órbitas izquierdas en M. El grupo $\mathcal{U}$ es el grupo de unidades de R, que es precisamente el grupo lineal general $GL_m(\mathbb{F}_q)$. Las órbitas izquierdas de $GL_m(\mathbb{F}_q)$ en $M = M_{m\times\ell}(\mathbb{F}_q)$ están representadas por la reducción escalonada por filas de las matrices sobre $\mathbb{F}_q$ de tamaño $m \times \ell$.

Ahora, es posible determinar $\mathcal{O}^\sharp$, el conjunto de las órbitas derechas $\operatorname{Aut}(A)$ en

$$\operatorname{Hom}_R(M, A).$$

El automorfismo de grupo $\operatorname{Aut}(A)$ es igual a $GL_k(\mathbb{F}_q)$, y actúa en $A = M_{m\times k}(\mathbb{F}_q)$ por medio de la multiplicación de matrices por la derecha. Por otra parte,

$$\operatorname{Hom}_R(M, A) = M_{\ell\times k}(\mathbb{F}_q),$$

nuevamente, por la multiplicación matricial por la derecha. Por lo tanto, $\mathcal{O}^\sharp$ consiste en las órbitas derechas de $GL_k(\mathbb{F}_q)$ que actúan en $M_{\ell\times k}(\mathbb{F}_q)$ de tamaño $\ell \times k$.

Puesto que la matriz transpuesta intercambia las filas escalonadas reducidas por las columnas escalonadas reducidas, se tiene que $\left|\mathcal{O}^{\sharp}\right| > |\mathcal{O}|$ si y sólo si $k > m$ (para cualquier ℓ positiva). Finalmente, $\dim_{\mathbb{Q}} F_0\left(\mathcal{O}^{\sharp}, \mathbb{Q}\right) > \dim_{\mathbb{Q}} F_0\left(\mathcal{O}, \mathbb{Q}\right)$ si y sólo si $m < k$. En consecuencia, si $m < k$, entonces W no es inyectiva y A no tiene la propiedad de extensión con respecto al peso de Hamming.

El aspecto técnico pendiente sobre la funcional cero es el siguiente. Para $\eta \in F\left(\mathcal{O}^{\sharp}, \mathbb{N}\right)$, se define la *longitud* de η como $l(\eta) = \sum_{\lambda \in \mathcal{O}^{\sharp}} \eta(\lambda)$ y la *longitud esencial* de η como $l_0(\eta) = \sum_{\lambda \neq 0} \eta(\lambda)$. La longitud $l(\eta)$ es igual a la longitud del código lineal definido por η; la longitud reducida $l_0(\eta)$ es igual a la longitud del código lineal definido por η luego de que cualquier posición igual con cero ha sido removida (en términos de una matriz generadora lo que se remueven son las columnas de ceros).

Si se asume que la propiedad de la extensión se verifica con respecto al peso de Hamming, significa que si $\eta, \eta' \in F\left(\mathcal{O}^{\sharp}, \mathbb{N}\right)$ satisface $l(\eta) = l(\eta')$ y $W_{\eta} = W_{\eta'}$, entonces $\eta = \eta'$. Esto es, W es inyectiva a lo largo de los niveles de la función de la longitud, l. Si $l(\eta') < l(\eta)$ y $W_{\eta} = W_{\eta'}$, entonces pueden agregarse ceros a η' hasta que su longitud sea la misma que $l(\eta)$ sin cambiar $W_{\eta'}$. De manera más precisa, definamos η'' como $\eta''(\lambda) = \eta'(\lambda)$ para $\lambda \neq 0$ y establezcamos $\eta''(0) = \eta'(0) + l(\eta) - l(\eta')$. Entonces, $l(\eta'') = l(\eta)$ y $W_{\eta''} = W_{\eta}$. Por la propiedad de la extensión, $\eta'' = \eta$. En particular, las longitudes reducidas son iguales: $l_0(\eta) = l_0(\eta') = l_0(\eta'')$.

Hay una proyección $\mathrm{pr} : F\left(\mathcal{O}^{\sharp}, \mathbb{N}\right) \to F_0\left(\mathcal{O}^{\sharp}, \mathbb{N}\right)$ que fija a $(\mathrm{pr}\,\eta)(0) = 0$ y deja a los valores restantes sin cambios, $(\mathrm{pr}\,\eta)(\lambda) = \eta(\lambda)$, $\lambda \neq 0$. Esta proyección divide el monoide como $F\left(\mathcal{O}^{\sharp}, \mathbb{N}\right) = F_0\left(\mathcal{O}^{\sharp}, \mathbb{N}\right) \oplus \mathbb{N}$. El argumento previo muestra que si $W_{\eta} = W_{\eta'}$, entonces $\mathrm{pr}\,\eta = \mathrm{pr}\,\eta'$ como elementos de $F_0\left(\mathcal{O}^{\sharp}, \mathbb{N}\right)$.

A la inversa, supongamos que $W : F_0\left(\mathcal{O}^{\sharp}, \mathbb{N}\right) \to F_0\left(\mathcal{O}, \mathbb{N}\right)$ es inyectivo. Sean η, $\eta' \in F\left(\mathcal{O}^{\sharp}, \mathbb{N}\right)$ tales que satisfacen $l(\eta) = l(\eta')$ y $W_{\eta} = W_{\eta'}$. Puesto que el valor de $\eta(0)$ no afecta a W_{η}, se tiene que $W_{\mathrm{pr}\,\eta} = W_{\mathrm{pr}\,\eta'}$. Por el supuesto, W es inyectiva en $F_0\left(\mathcal{O}^{\sharp}, \mathbb{N}\right)$ de forma que $\mathrm{pr}\,\eta = \mathrm{pr}\,\eta'$. En particular, $l_0(\eta) = l_0(\eta')$. Dado que $l(\eta) = l(\eta')$, se sigue que $\eta(0) = \eta'(0)$ y por lo tanto $\eta = \eta'$.

Capítulo 2

Álgebras de Hopf

Desde su introducción, las álgebras de Hopf han sido estudiadas por muchos matemáticos. En los inicios de 1970, Hochschild [28], mientras desarrollaba la teoría de grupos algebraicos, tradujo gran parte de la teoría de la representación al lenguaje de las álgebras de Hopf. Por ejemplo, [60] es un clásico con esta perspectiva, mientras que en [26] se cuenta con un texto más moderno al respecto. En cierto sentido, puede decirse que las álgebras de Hopf brindaron a los matemáticos un nuevo marco para desarrollar la teoría de la representación ya que desde la publicación del libro de Sweedler [68] hubo una serie de esfuerzos por probar resultados conocidos para grupos afines, e incluso hallar nuevos, empleando métodos propios de las álgebras de Hopf (ejemplos de ello se encuentran en [66, 67] y [70, 71]).

En este capítulo se expone la definición formal de álgebra de Hopf y se presentan resultados fundamentales en el desarrollo de la teoría, mayormente provistos por Montgomery [54] a menos que se indique lo contrario. El resultado principal de este capítulo se debe a Larson y Sweedler [47], quienes probaron que toda álgebra de Hopf de dimensión finita es de Frobenius. Al ser los grupos cuánticos ejemplos de álgebras de Hopf, este resultado revela que éstos representan un campo fértil para la Teoría de Códigos ya que -como se mostró en el capítulo previo- todo anillo de Frobenius finito tiene la propiedad de la extensión para el peso de Hamming y, a la vez, todo anillo finito que verifica esta propiedad debe ser de Frobenius.

2.1. Álgebras y coálgebras

En adelante, **k** denotará un campo, aun cuando los temas que abordaremos a lo largo del presente capítulo son también válidos sobre cualquier anillo conmutativo.

2.1 Definición. Sean V y W dos espacios vectoriales cualesquiera sobre un campo **k**. El *producto tensorial* de V y W, denotado como $V \otimes W$, es el espacio de elementos tales que

$$v_1 \otimes w_1 + v_2 \otimes w_2 + \cdots + v_n \otimes w_n$$

donde $v_i \in V$, $w_i \in W$ y con las siguientes relaciones bilineales:

$$a_1 (v_1 \otimes w) + a_2 (v_2 \otimes w) = ((a_1 v_1 + a_2 v_2) \otimes w)$$

y

$$a_1 (v \otimes w_1) + a_2 (v \otimes w_2) = (v \otimes (a_1 w_1 + a_2 w_2))$$

donde $a_i \in \mathbf{k}$, $v, v_i \in V$ y $w, w_i \in W$.

Los productos tensoriales se asumirán sobre **k** a menos que se indique lo contrario. Cabe destacar que si B_V es una base para V y B_W es una base para W, entonces

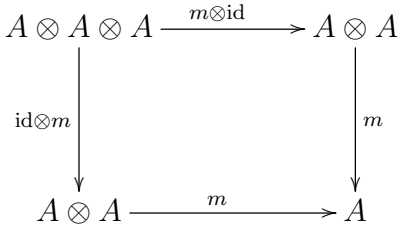
$$B_{V \otimes W} = \{e \otimes f | e \in B_V \text{ y } f \in B_W\}$$

es una base para $V \otimes W$.

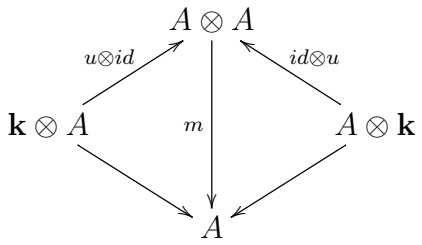
Ahora que hemos introducido los elementos fundamentales anteriores, expresaremos primero las propiedades asociativa y de unidad de una álgebra por medio de mapeos, de forma que podamos dualizarlos.

2.2 Definición. Una **k**-álgebra (con unidad) es un espacio vectorial A con dos mapeos lineales: la multiplicación $m : A \otimes A \to A$ y la unidad $u : \mathbf{k} \to A$, tales que los siguientes diagramas son conmutativos:

i) Asociatividad:



ii) Unidad:



Los dos mapeos inferiores en *ii*) están dados por la multiplicación por un escalar. En la Definición 2.2, *ii*) se desprende el elemento identidad en A, haciendo $1_A = u(1_{\mathbf{k}})$.

2.3 Definición. Sean A y B álgebras y m_A, m_B sus respectivas multiplicaciones. El mapeo lineal $g : A \to B$ es un *morfismo de álgebras* si $g \circ m_A = m_B \circ (g \otimes g)$, es decir, si el siguiente diagrama conmuta:

$$\begin{array}{ccc} A \otimes A & \xrightarrow{m_A} & A \\ {\scriptstyle g\otimes g}\downarrow & & \downarrow{\scriptstyle g} \\ B \otimes B & \xrightarrow{m_B} & B \end{array}$$

Dicho de otro modo, la definición de un morfismo de álgebras implica que $g(ab) = g(a)\, g(b)$.

2.4 Definición. Para dos $\mathbf{k}$-espacios cualesquiera V y W, el *mapeo torcido* $\tau : V \otimes W \to W \otimes V$ está dado por $\tau(v \otimes w) = w \otimes v$.

Notemos que A es conmutativa si y sólo si $m \circ \tau = m$ en $A \otimes A$.

A continuación dualizaremos la noción de álgebra.

2.5 Definición. Una $\mathbf{k}$-coálgebra (con counidad) es un $\mathbf{k}$-espacio vectorial C junto con dos $\mathbf{k}$-mapeos lineales, la *comultiplicación* o *coproducto* $\Delta : C \to C \otimes C$ y la *counidad* $\epsilon : C \to \mathbf{k}$, tales que los siguientes diagramas conmutan:

i) Coasociatividad:

$$\begin{array}{ccc} C & \xrightarrow{\Delta} & C \otimes C \\ {\scriptstyle \Delta}\downarrow & & \downarrow{\scriptstyle \Delta\otimes id} \\ C \otimes C & \xrightarrow{id\otimes\Delta} & C \otimes C \otimes C \end{array}$$

ii) Counidad:

$$\begin{array}{ccccc} & & C & & \\ & {\scriptstyle 1\otimes}\swarrow & \downarrow{\scriptstyle \Delta} & \searrow{\scriptstyle \otimes 1} & \\ \mathbf{k} \otimes C & & & & C \otimes \mathbf{k} \\ & {\scriptstyle id\otimes\epsilon}\nwarrow & \downarrow & \nearrow{\scriptstyle \epsilon\otimes id} & \\ & & C \otimes C & & \end{array}$$

Los dos mapeos superiores de la counidad en la Definición 2.5, están dados por $c \mapsto 1 \otimes c$

y $c \mapsto c \otimes 1$ para toda $c \in C$. Se dice que C es *coconmutativa* si $\tau \circ \Delta = \Delta$.

Puesto que en el caso de la unidad en la Definición 2.2 el mapeo m es suprayectivo, se sigue que para la counidad el mapeo Δ es inyectivo.

2.6 Definición. Sean C y D coálgebras con comultiplicaciones Δ_C y Δ_D y counidades ϵ_C y ϵ_D, respectivamente.

i) Un mapeo $f : C \to D$ es un *morfismo de coálgebras* si $\Delta_D \circ f = (f \otimes f)\,\Delta_C$ y si $\epsilon_C = \epsilon_D \circ f$.

ii) Un subespacio $I \subseteq C$ es un *coideal* si $\Delta I = I \otimes C + C \otimes I$ y si $\epsilon\,(I) = 0$.

Si I es un coideal, entonces el $\mathbf{k}$-espacio generado por C/I es una coálgebra con comultiplicación inducida por Δ y viceversa.

Ahora, emplearemos el mapeo torcido para dualizar la noción de una álgebra opuesta. Para una álgebra dada A, A^{op} denota el álgebra obtenida usando A como espacio vectorial pero con una nueva multiplicación $a^\circ \cdot b^\circ = (ba)^\circ$, para $a^\circ, b^\circ \in A^{op}$. En términos de mapeos, esta nueva multiplicación está dada por $m' : A \otimes A \to A$, donde $m' = m \circ \tau$.

2.7 Definición. Sea C una coálgebra. Entonces, la *coálgebra coopuesta* C^{cop} está definida como sigue: $C^{cop} = C$ como espacio vectorial, con nueva comultiplicación Δ' dada por $\Delta' = \tau \circ \Delta$.

Una observación importante es que C^{cop} es también una coálgebra.

Ahora estudiaremos la estrecha relación que hay entre álgebras y coálgebras, mediante sus respectivos espacios duales.

Para todo $\mathbf{k}$-espacio V, sea $V^* = \mathrm{Hom}_{\mathbf{k}}\,(V, \mathbf{k})$ el dual lineal de V. V y V^* determinan una forma bilineal no degenerada $\langle , \rangle : V^* \otimes V \to \mathbf{k}$ tal que $\langle f, v \rangle = f(v)$; esta notación se debe a que generalmente se concibe a V actuando sobre V^*. Si $\phi : V \to W$ es $\mathbf{k}$-lineal, entonces la *transpuesta* de ϕ es $\phi^* : W^* \to V^*$, dada por

$$\phi^*\,(f)\,(v) = f\,(\phi\,(v))\,,$$

para toda $f \in W^*$ y $v \in V$.

2.8 Lema. *Si C es una coálgebra, entonces C^* es una álgebra, con multiplicación $m = \Delta^*$ y unidad $u = \epsilon^*$. Si C es coconmutativa, entonces C^* es conmutativa.*

La demostración del lema anterior consiste en dualizar los diagramas. Sólo se requiere observar que, puesto que $C^* \otimes C^* \subseteq (C \otimes C)^*$, debe restringirse Δ^* para obtener un mapeo $m : C^* \otimes C^* \to C^*$. Explícitamente, m está dada por $m(f \otimes g)(c) = \Delta^*(f \otimes g)(c) = (f \otimes g)\Delta_C$ para toda $f, g \in C^*$ y $c \in C$.

Sin embargo, si comenzamos con una álgebra A habrá una serie de dificultades. Por ejemplo, si A no es de dimensión finita, $A^* \otimes A^*$ es un subespacio propio de $(A \otimes A)^*$ en cuyo caso la imagen de $m^* : A^* \to (A \otimes A)^*$ puede no encontrarse en $A^* \otimes A^*$. Por supuesto, si A es de dimensión finita no habrá mayor problema y A^* será una coálgebra. Para el caso general se requiere de una nueva definición.

2.9 Definición. Sea A una **k**-álgebra. El *finito dual* de A es

$$A^o = \{f \in A^* | f(I) = 0, \text{ para algún ideal } I \text{ de } A \text{ tal que } \dim(A/I) < \infty\}.$$

2.10 Proposición. *Si A es una álgebra, entonces A^o es una coálgebra, con comultiplicación $\Delta = m^*$ y counidad $\epsilon = u^*$. Si A es conmutativa, entonces A^o es coconmutativa.*

De forma explícita, $\Delta f(a \otimes b) = m^* f(a \otimes b) = m^* f(a \otimes b) = f(ab)$, para toda $f \in A^o$ y $a, b \in A$.

La demostración detallada de 2.10 se encuentra en [54]. En particular, A^o es el mayor subespacio V de A^* tal que $m^*(V) \subseteq V \otimes V$.

2.2. Biálgebras, convolución y antípodas

Ahora se combinarán las nociones de álgebra y coálgebra para dar paso a una nueva estructura.

2.11 Definición. Un **k**-espacio B es una *biálgebra* si (B, m, u) es una álgebra, (B, Δ, ϵ) es una coálgebra y cualesquiera de las siguientes condiciones equivalentes se satisface:

i) Δ y ϵ son morfismos de álgebras.

ii) m y u son morfismos de coálgebras.

Generalmente, y bajo la notación recién expuesta, la estructura de una biálgebra se denota por $(B, m, u, \Delta, \epsilon)$. Como es de esperarse, el mapeo $f : B \to B'$ de biálgebras se llama *morfismo de biálgebras* si es tanto un morfismo de álgebras como un morfismo de coálgebras. Un subespacio $I \subseteq B$ es un *biideal* si es tanto un ideal como un coideal. El cociente B/I es una biálgebra precisamente cuando I es un biideal de B.

2.12 Definición. Sea C cualquier coálgebra y $c \in C$.

i) Se dice que c es de *tipo grupo* si $\Delta(c) = c \otimes c$ y si $\epsilon(c) = 1$. El conjunto de elementos de tipo grupo en C se denota por $G(C)$.

ii) Para $g, h \in G(C)$, se dice que c es *h-primitivo* de g si $\Delta(c) = c \otimes g + h \otimes c$. Al conjunto de todos los elementos *h-primitivos* de g se le denota como $P_{h,g}(C)$. Si $C = B$ es una biálgebra y $g = h = 1$, entonces a los elementos $P(B) = P_{1,1}(B)$ se les llama simplemente como *elementos primitivos* de B.

Antes de introducir la definición de álgebra de Hopf, presentaremos una nueva definición y una notación muy útil.

2.13 Definición. Sea C una coálgebra y A una álgebra. Entonces $\mathrm{Hom}_{\mathbf{k}}(C, A)$ se convierte en una álgebra bajo el *producto convolución*

$$(f * g)(c) = m \circ (f \otimes g) \Delta(c)$$

para toda $f, g \in \mathrm{Hom}_{\mathbf{k}}(C, A)$, $c \in C$. El elemento unitario en $\mathrm{Hom}_{\mathbf{k}}(C, A)$ es $u(\epsilon)$.

Más adelante se brindará una fórmula que permite calcular con facilidad $f * g$.

Notemos que ya hemos visto un ejemplo de convolución previamente; para cualquier coálgebra C, la multiplicación $m = \Delta^*$ en $C^* = \mathrm{Hom}(C, \mathbf{k})$ (véase Lema 2.8).

Puede definirse también el producto *convolución torcido* en $\mathrm{Hom}_{\mathbf{k}}(C, A)$ (anticonvolución), por medio de

$$(f \times g)(c) = m \circ (f \otimes g)(\tau \circ \Delta(c)).$$

En el caso de las álgebras, la multiplicación produce una disminución en el número de elementos de una expresión. Por ejemplo, a partir de la multiplicación de dos elementos

se obtiene sólo un nuevo elemento. En cambio, la comultiplicación en las coálgebras produce el efecto contrario: al aplicar el coproducto a un elemento se obtiene una familia finita de pares de elementos. Por esta razón, los cálculos en una coálgebra son, en general, más complejos de llevar a cabo que en el caso de una álgebra. La siguiente notación, introducida por Heyneman y Sweedler, resulta particularmente útil para simplificar esta tarea.

2.14 Definición. Sea C cualquier coálgebra con comultiplicación $\Delta : C \to C \otimes C$. La *notación sigma* de Δ es la siguiente: para toda $c \in C$, el coproducto se escribe como

$$\Delta(c) = \sum c_{(1)} \otimes c_{(2)}.$$

Los subíndices (1) y (2), en la definición anterior son simbólicos y no representan elementos particulares de C. Esta notación es análoga a la empleada en física (en la que incluso se omite la $\sum$).

La relevancia en el empleo de esta notación se pone de manifiesto cuando Δ debe ser aplicada más de una vez. En particular, de la coasociatividad en el diagrama $i)$ de la Definición 2.5 se tiene que

$$\sum c_{(1)} \otimes c_{(2)_{(1)}} \otimes c_{(2)_{(2)}} = \sum c_{(1)_{(1)}} \otimes c_{(1)_{(2)}} \otimes c_{(2)};$$

este elemento se escribe como

$$\sum c_{(1)} \otimes c_{(2)} \otimes c_{(3)} = \Delta_2(c).$$

Realizando este proceso de forma iterativa, se sigue que

$$\Delta_{n-1}(c) = \sum c_{(1)} \otimes \ldots \otimes c_{(n)}$$

donde $\Delta_{n-1}(c)$ es necesariamente el único elemento obtenido al aplicar la coasociatividad $n-1$ veces.

Con esta notación, el diagrama de la counidad (Definición 2.5) establece que para toda $c \in C$,

$$c = \sum \epsilon\left(c_{(1)}\right) c_{(2)} = \sum \epsilon\left(c_{(2)}\right) c_{(1)}$$

y que la convolución se calcula como

$$(f * g)(c) = \sum f\left(c_{(1)}\right) g\left(c_{(2)}\right).$$

2.15 Definición. Sea $H\,(H, m, u, \Delta, \epsilon)$ una biálgebra. Se dice que H es una *álgebra de Hopf* si existe un elemento $S \in \mathrm{Hom}_{\mathbf{k}(H,H)}$ que sea inverso a id_H bajo una convolución $*$. S es llamada la *antípoda* de H.

Se observa que, en notación sigma, S satisface que

$$\sum (Sh_1)\, h_2 = \epsilon(h)\, 1_H = \sum h_1\, (Sh_2) \tag{2.1}$$

para toda $h \in H$.

Las nociones de morfismos e ideales para esta nueva estructura se exponen a continuación. El mapeo $f : H \to K$ de álgebras de Hopf es un *morfismo de Hopf* si es un morfismo de biálgebras y $f(S_H h) = S_K f(h)$, para toda $h \in H$. Un subespacio I de H es un *ideal de Hopf* si es un biideal y si $SI \subseteq I$; en esta situación H/I es una álgebra de Hopf con estructura inducida por H.

Las siguientes son algunas propiedades importantes de la antípoda.

2.16 Proposición. *Sea H una álgebra de Hopf con S como antípoda. Entonces,*

i) *S es un* morfismo de antiálgebras*; esto es*

$$S(hk) = S(k)\, S(h),$$

donde $h, k \in H$ y $S(1) = 1$.

ii) *S es un* morfismo de anticoálgebras*; esto es*

$$\Delta \circ S = \tau \circ (S \otimes S) \circ \Delta$$

y $\epsilon \circ S = \epsilon$.

En notación sigma, *ii)* significa que $\sum (Sh_1) \otimes (Sh_2) = (Sh_2) \otimes (Sh_1)$.

Recordemos que para una biálgebra B, B^{cop} es la biálgebra con comultiplicación opuesta. B^{cop} es una álgebra de Hopf con antípoda $\bar{S}$ en donde esta última es la inversa de id_H bajo la convolución torcida definida enseguida de la Definición 2.13. Esto es, $\sum \left(\bar{S}h_2\right) h_1 = \sum h_2 \left(\bar{S}h_1\right) = \epsilon(h)\, 1$, para toda $h \in B$. Por la Proposición 2.16 aplicada a B^{cop}, se sigue que $\bar{S}$ es un morfismo de antiálgebras, pero también un morfismo de anticoálgebras. Se llama a $\bar{S}$ la *antípoda torcida* de B.

2.17 Lema. *Sea B una biálgebra. Entonces B es una álgebra de Hopf con (composición) antípoda invertible S si, y sólo si, B^{cop} es una álgebra de Hopf con (composición) antípoda invertible $\bar{S}$. En este contexto, $S \circ \bar{S} = \bar{S} \circ S = \mathrm{id}$ y entonces $\bar{S} = S^{-1}$.*

Demostración. Asumamos que S' es una composición inversa para S; entonces S' es también un antiautomorfismo de B. Ahora, para toda $b \in B$,

$$\sum (S'b_2)\, b_1 = \sum (S'b_2)\, (S'Sb_1) = S'\left(\sum (Sb_1)\, b_2\right) = S'\left(\epsilon\,(b)\, 1\right) = \epsilon\,(b)\, 1.$$

Esto es, $S' \times \mathrm{id} = u\epsilon$. De manera similar, $\mathrm{id} \times S' = u\epsilon$, y entonces S' es una antípoda para B^{cop}.

Ahora, asumamos que B tiene tanto una S como una $\bar{S}$ y elijamos $b \in B$. Entonces,

$$\begin{array}{lll} \bar{S}Sb & = \sum \bar{S}S\,(\epsilon\,(b_2)\, b_1) & = \sum \epsilon\,(b_2)\, \bar{S}Sb_1 \quad = \sum b_3\left(\bar{S}b_2\right) \bar{S}Sb_1 \\ & = \sum b_3 \bar{S}\,((Sb_1)\, b_2) & = \sum b_2 \bar{S}\,(\epsilon\,(b_1)) \quad = \sum \epsilon\,(b_1)\, b_2 = b. \end{array}$$

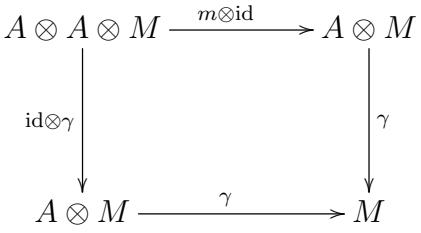
Así, $\bar{S} \circ S = \mathrm{id}$ y, de manera similar, $S \circ \bar{S} = \mathrm{id}$. □

2.3. Módulos y comódulos

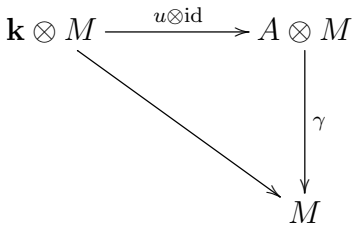
Así como hicimos en el caso de las álgebras, primero consideraremos la definición de módulo y enseguida introduciremos el concepto de comódulo.

2.18 Definición. Para una $\mathbf{k}$-álgebra A, un *A-módulo izquierdo* es un $\mathbf{k}$-espacio M con un mapeo $\mathbf{k}$-lineal $\gamma : A \otimes M \to M$ tal que los siguientes diagramas conmutan:

i)



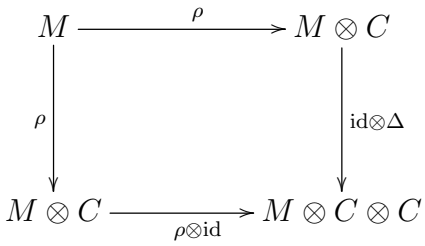
ii)

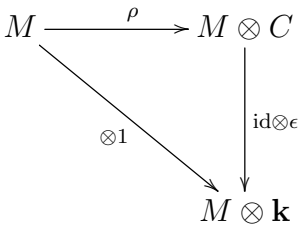


La categoría de A-módulos izquierdos se denota como ${}_A\mathcal{M}$.

2.19 Definición. Para una **k**-coálgebra C, un *C-comódulo derecho* es un **k**-espacio M con un mapeo **k**-lineal $\rho : M \to M \otimes C$ tal que los siguientes diagramas conmutan:

i) **ii)**





La categoría de C-comódulos derechos se denota como $\mathcal{M}^C$.

También existe una notación sigma para comódulos de derecha: se escribe

$$\rho(m) = \sum m_{(0)} \otimes m_{(1)} = \sum m_0 \otimes m_1 \in M \otimes C,$$

preservando la convención de que $m_{(i)} \in C$ para $i \neq 0$. De forma análoga, se tienen comódulos izquierdos por medio del mapeo $\rho' : M \to C \otimes M$, y se emplea la notación

$$\rho'(m) = \sum m_{(-1)} \otimes m_{(0)} = \sum m_{-1} \otimes m_0.$$

2.20 Definición. Sean M y N C-comódulos derechos con mapeos estructurales ρ_M y ρ_N, respectivamente. El mapeo $f : M \to N$ es un *morfismo de comódulos* si $\rho_N \circ f = (f \otimes \mathrm{id}) \circ \rho_M$.

Aquí, como en la sección §2.1, existe una fuerte conexión entre módulos y comódulos.

2.21 Lema. i) *Si M es un C-comódulo derecho, entonces M es un C^*-módulo.*

ii) *Sea M un A-módulo izquierdo. Entonces M es un A^o-comódulo derecho si, y sólo si, $\{A \cdot m\}$ es de dimensión finita, para toda $m \in M$.*

Demostración. **i)** Si $\rho : M \to M \otimes C$ es el mapeo comodular, con $\rho(m) = \sum m_0 \otimes m_1$, y $f \in C^*$, entonces M se convierte en un C^*-módulo a través de

$$f \cdot m = \sum \langle f, m_1 \rangle m_0.$$

ii) Elijamos $m \in M$ y sea $\{m_1, \ldots, m_n\}$ una base para $A \cdot m$. Entonces, para toda $a \in A$, $a \cdot m = \sum_{i=1}^{n} f_i(a)\, m_i$, para alguna $f_i(a) \in \mathbf{k}$. Ahora $I = \ker(A \to \mathrm{End}_{\mathbf{k}}(A \cdot m))$ es un ideal de dimensión cofinita de A, en la que f_i se desvanece. Así, $f_i \in A^o$, para toda $i = 1, \ldots, n$. Entonces M se convierte en un A^o-comódulo a través del mapeo $\rho : M \to M \otimes A^o$, $m \mapsto \sum_i m_i \otimes f_i$.

Ahora bien, por i), $A \cdot m$ está generado por el conjunto m_0 en $\rho(m)$.

□

En general, la inversa de i) es falsa, es decir, no todos los C^*-módulos izquierdos son también C-comódulos. Un C^*-módulo M que se convierte en un C-comódulo de manera natural adquiere el nombre de *racional*.

Un subcomódulo derecho D de C es un subespacio tal que $\Delta(D) \subseteq D \otimes C$; D se llama *coideal derecho* de C. De manera similar, un subcomódulo izquierdo E es un subespacio tal que $\Delta(E) \subseteq C \otimes E$ y es llamado *coideal izquierdo*.

Por otra parte, la acción de una álgebra de Hopf en el producto tensorial de módulos se extiende a la acción diagonal usual para grupos.

2.22 Definición. Sea H una álgebra de Hopf; y V y W, H-módulos izquierdos. Entonces $V \otimes W$ es también un H-módulo izquierdo por medio de

$$h \cdot (v \otimes w) = \sum (h_1 \cdot v) \otimes (h_2 \cdot w)$$

para toda $h \in H$, $v \in V$ y $w \in W$.

De manera similar, el producto tensorial de H-módulos derechos es nuevamente un H-módulo derecho.

Cuando H es coconmutativo, entonces $V \otimes W \cong W \otimes V$, extendiendo de nueva cuenta lo que se ha mencionado para grupos. Sin embargo, en general no se verifica que $V \otimes W \cong W \otimes V$ como H-módulos. Como contraejemplo, podemos considerar $H = (\mathbf{k}G)^*$ para cualquier grupo abeliano finito G.

Cuando se tiene una biálgebra de dimensión finita -esto es, cuando $|G| < \infty$- puede plantearse $\{p_x | x \in G\}$ como base de $(\mathbf{k}G)^*$ dual a la base de los elementos de tipo grupo

en $\mathbf{k}G$; es decir, $p_x(y) = \delta_{x,y}$, todas $x, y \in G$. Entonces,

$$\Delta p_x = \sum_{uv=x} p_u \otimes p_v. \tag{2.2}$$

Si se eligen $g, h \in G$ con $gh \neq hg$, y se tiene que $V = \mathbf{k}p_g$, $W = \mathbf{k}p_h$, entonces $p_{gh} \cdot (V \otimes W) \neq 0$, pero $p_{gh} \cdot (W \otimes V) = 0$, haciendo uso de (2.2).

La Definición 2.22 puede reescribirse en término de mapeos. Así, si $\phi_V : H \otimes V \to V$ y $\phi_W : H \otimes W \to W$ son las dos acciones de módulo dadas, entonces

$$\phi_{V\otimes W} = (\phi_V \otimes \phi_W) \circ (\mathrm{id} \otimes \tau \otimes \mathrm{id}) \circ \left(\Delta \otimes \mathrm{id}^2\right) : H \otimes V \otimes V \otimes W \to V \otimes W.$$

Al dualizar esta definición, se obtiene la siguiente:

2.23 Definición. Sea H una álgebra de Hopf; y V y W, H-comódulos derechos con mapeos estructurales ρ_V y ρ_W, respectivamente. Entonces $V \otimes W$ es también un H-comódulo derecho a través de

$$\rho_{V\otimes W} = (\mathrm{id} \otimes m) \circ (\mathrm{id} \otimes \tau \otimes \mathrm{id}) \circ (\rho_V \otimes \rho_W) : V \otimes W \to V \otimes W \otimes H.$$

En términos de elementos, tenemos que $\rho(v \otimes w) = \sum v_0 \otimes w_0 \otimes v_1 w_1$.

Enseguida nos referiremos a conceptos propios de una álgebra de Hopf H que serán útiles más adelante, al probar el resultado principal de este capítulo.

2.24 Definición. i) Sea M un H-módulo izquierdo. Los *invariantes* de H en M son el conjunto

$$M^H = \{m \in M | h \cdot m = \epsilon(h)\, m, \text{ para toda } h \in H\}.$$

ii) Sea M un H-comódulo derecho. Los *coinvariantes* de H en M es el conjunto

$$M^{coH} = \{m \in M | \rho(m) = m \otimes 1\}.$$

Para distinguir ente invariantes izquierdos y derechos, la notación en $i)$ de la Definición 2.24 puede adaptarse a ${}^H M$. Sin embargo, la notación estándar para invariantes es M^H, sin importar si son derechos o izquierdos.

El siguiente lema resulta de las construcciones en la demostración del Lema 2.21.

2.25 Lema. i) *Sea M un H-comódulo derecho, y consideremos su estructura H^*-modular izquierda. Entonces $M^{H^*} = M^{coH}$.*

ii) *Sea M un H-módulo izquierdo tal que es también un H^o-comódulo derecho. Entonces $M^H = M^{coH^o}$.*

2.4. Módulos de Hopf

Así como una álgebra de Hopf es tanto una álgebra como una coálgebra, un módulo de Hopf es tanto un módulo como un comódulo.

2.26 Definición. Para una **k**-álgebra de Hopf H, un *H-módulo de Hopf derecho* es un **k**-espacio M tal que

i) M es un H-módulo derecho;

ii) M es un H-comódulo derecho por medio de $\rho : M \to M \otimes H$;

iii) ρ es un mapeo del H-módulo derecho, donde $M \otimes H$ es un H-módulo derecho como en 2.23, y donde H actúa sobre sí mismo por medio de la multiplicación por la derecha.

Podemos escribir *iii)* como $\sum (m \cdot h)_0 \otimes (m \cdot h)_1 = \sum m_0 \cdot h_1 \otimes m_1 h_2$, para toda $m \in M$ y $h \in H$.

De manera más general, en la parte modular de la definición podemos reemplazar H por cualquier subálgebra de Hopf K de H; de tal suerte, M se convierte en un (H, K)-módulo de Hopf derecho. La categoría de todos los (H, K)-módulos de Hopf derechos se denota como $\mathcal{M}_K^H$.

Claramente, podemos reemplazar también la acción por la derecha por una acción izquierda, obteniendo tres categorías adicionales de (H, K)-módulos de Hopf: ${}^H\mathcal{M}_K$, ${}_K\mathcal{M}^H$ y ${}^H_K\mathcal{M}$.

El siguiente resultado es de particular importancia.

2.27 Teorema (Teorema fundamental de los módulos de Hopf)**.** *Sea $M \in \mathcal{M}_H^H$. Entonces $M \cong M^{coH} \otimes H$ como H-módulos de Hopf derechos, donde $M^{coH} \otimes H$ es un módulo de Hopf trivial.*

En particular, M es un H-módulo derecho libre de rango igual a $\dim_{\mathbf{k}} M^{coH}$.

Demostración. La demostración del teorema es extensa y puede consultarse a detalle en [68]. A continuación se hará una breve descripción de la misma.

Definamos $\alpha : M^{coH} \otimes H \to M$ como $m' \otimes h \mapsto m' \cdot h$ y $\beta : M \to M \otimes H$ como $m \mapsto \sum m_0 \cdot (Sm_1) \otimes m_2$.

Primero, debe mostrarse que $\beta(M) \subseteq M^{coH} \otimes H$ al ser $\rho(\sum m_0 \cdot Sm_1) = \sum m_0 \cdot Sm_1 \otimes 1$, es decir, $\sum m_0 \cdot (Sm_1) \in M^{coH}$. Para ello se requiere usar *iii*) de la Definición 2.26. Enseguida, se verifica que $\alpha\beta = \mathrm{id}$ y $\beta\alpha = \mathrm{id}$.

Finalmente, debe verificarse que α es un mapeo H-comodular derecho, nuevamente haciendo uso de *iii*) en la Definición 2.26; de forma que α es un mapeo H-modular derecho. Así, α es un isomorfismo de H-módulos de Hopf. □

Una demostración muy similar funciona para cualquier H-módulo de Hopf izquierdo $M \in_H^H \mathcal{M}$. Sin embargo, para los módulos «híbridos» en ${}^H\mathcal{M}_H$ o ${}_H\mathcal{M}^H$, se requiere que H cuente con una antípoda torcida $\bar{S}$. Por ejemplo, si $M \in_H \mathcal{M}^H$, entonces el mapeo β en el Teorema 2.27 es reemplazado por $\beta' : M \to M \otimes H$ dado por $m \mapsto \sum \left(\bar{S}m_1\right) \cdot m_0 \otimes m_2$. Así, $M \cong M^{coH} \otimes H$, como anteriormente.

Para concluir esta sección se presentarán los argumentos necesarios para demostrar el teorema de Larson y Sweedler, cuya importancia radica en que establece la relación entre álgebras de Hopf finitas y álgebras de Frobenius.

2.28 Definición. Una *integral izquierda* en H es un elemento $t \in H$ tal que $ht = \epsilon(h)\, t$, para toda $h \in H$; una *integral derecha* en H es un elemento $t' \in H$ tal que $t'h = \epsilon(h)\, t'$, para toda $h \in H$.

$\int_H^l$ denota el espacio de integrales izquierdas; y $\int_H^r$, el espacio de integrales derechas. H se llama *unimodular* si $\int_H^l = \int_H^r$.

2.29 Teorema. *Sea H cualquier álgebra de Hopf de dimensión finita. Entonces*

i) $\int_H^l$ *y* $\int_H^r$ *son cada una unidimensional;*

ii) *la antípoda* S *de* H *es biyectiva, y* $S\left(\int_H^\ell\right) = \int_H^r$*;*

iii) H *es un* H^**-módulo izquierdo y derecho cíclico;*

iv) H *es una álgebra de Frobenius.*

Recordemos que A es una álgebra de Frobenius si existe una forma bilineal asociativa no degenerada $(,) : A \otimes A \to \mathbf{k}$.

A pesar de que existen otras pruebas para el teorema, en esta ocasión se presenta la demostración basada en el Teorema fundamental de módulos de Hopf. El esbozo de ésta es el siguiente:

Primero debe mostrarse que $M = H^*$ se convierte en un H-módulo de Hopf derecho al emplear una acción y una coacción particular. Primero, H^* es un H^*-módulo izquierdo por medio de la multiplicación por la izquierda y se convierte en un H-comódulo como en el Lema 2.21. Esto es, si $\{g_1, \ldots, g_n\}$ es una base de H^* y $f \in H^*$, entonces existen $h_1, h_2, \ldots, h_n \in H$ tales que para cualquier $g \in H^*$, $gf = \sum_i \langle g, h_i \rangle g_i$. El mapeo de comódulos $\rho : H^* \to H^* \otimes H$ está dado por $\rho(f) = \sum_i gi \otimes h_i$. A la inversa, si $\rho(f) = \sum f_0 \otimes f_1$, entonces $gf = \sum \langle g, f_1 \rangle f_0$.

Por otra parte, H^* es también un H módulo derecho por medio de $\leftharpoonup$: si $f \in H^*$, y $h, \ell \in H$, entonces $\langle f \leftharpoonup h, \ell \rangle = \langle f, \ell (Sh) \rangle$.

2.30 Lema. $M = H^* \in \mathcal{M}_H^H$ *al emplear* ρ *y* $\leftharpoonup$ *como arriba.*

Demostración. Primero, se requiere que

$$g(f \leftharpoonup h) = \sum ((h_2 \rightharpoonup g) f) \leftharpoonup h_1 \tag{2.3}$$

para toda $f, g \in H^*$ y $h \in H$. Esto se sigue del hecho de que H^* es una «álgebra de H-modular» bajo $\leftharpoonup$ (esto es, $h \rightharpoonup fg = \sum (h_1 \leftharpoonup f)(h_2 \rightharpoonup g)$).

Para demostrar que $H^* \in \mathcal{M}_H^H$ debe mostrarse que ρ es un H-mapeo derecho, es decir, $\rho(f \leftharpoonup h) = \sum (f_0 \leftharpoonup h_1) \otimes f_1 h_2 = \rho(f) \cdot h$. Esto equivale a probar que

$$g(f \leftharpoonup h) = \sum \langle g, f_1 h_2 \rangle (f_0 \leftharpoonup h_1),$$

para todas $f, g \in H^*$, $h \in H$. Al emplear (2.3) se obtiene

$$\begin{aligned} g\left(f \leftharpoonup h\right) &= \sum \left(\left(h_2 \rightharpoonup g\right) f\right) \leftharpoonup h_1 \\ &= \sum \left[\left\langle h_2 \rightharpoonup g, f_1 \right\rangle f_0\right] \leftharpoonup h_1 \\ &= \sum \left\langle h_2 \rightharpoonup g, f_1 \right\rangle \left(f_0 \leftharpoonup h_1\right) \\ &= \sum \left\langle g, f_1 h_2 \right\rangle \left(f_0 \leftharpoonup h_1\right). \end{aligned}$$

□

A continuación, la demostración del teorema.

Demostración (del Teorema de Larson-Sweedler). **i)** Por el lema anterior, $M = H^* \in \mathcal{M}_H^H$ y entonces $M \cong M^{coH} \otimes H$ por el Teorema fundamental de módulos de Hopf. Dado que $\dim M^* = \dim H^* = \dim H$, se sigue que $\dim M^{coH} = 1$. Pero, por el Lema 2.25

$$\left(H^*\right)^{coH} = \left(H^*\right)^{H^*} = \left\{f \in H^* | gf = \epsilon_{H^*}(g) f, \text{ para toda } g \in H^*\right\}.$$

Por lo tanto, $\dim \int_{H^*}^l = 1$. Al reemplazar H por H^* queda demostrado i).

ii) Elijamos $0 \neq f \in \int_{H^*}^l$. Si $h \in \ker S$, entonces $\alpha\left(f \otimes h\right) = Sh \rightharpoonup f = 0$, donde α es el mapeo expuesto en la demostración del Teorema fundamental. Puesto que α es inyectiva, $f \otimes h = 0$, y entonces $h = 0$. Así, S es inyectiva. Como H es de dimensión finita, es biyectiva. Así, $S\left(\int_H^\ell\right) = \int_H^r$, y por lo tanto $\int_H^r$ tiene también dimensión uno.

iii) Nuevamente, usando α como en ii), $f \otimes H \cong H^*$. Así, $H^{ast} = f \leftharpoonup H = SH \rightharpoonup f = H \rightharpoonup f$, al emplear ii) para la última igualdad. Al dualizar se obtiene el resultado deseado.

iv) Elijamos de nuevo $0 \neq f \in \int_{H^*}^l$ y definamos $(h, k) = \langle f, hk \rangle \in \mathbf{k}$. Esta forma es asociativa y bilineal. Para verificar que es no degenerada, es suficiente con probarlo por la izquierda puesto que H es de dimensión finita. Asumamos que para alguna $a \in H$, $(a, H) = 0$. Entonces, $0 = \langle f, aH \rangle = \langle H \rightharpoonup f, a \rangle = \langle H^*, a \rangle$ por medio de iii) y la definición de $\rightharpoonup$. Esto es, $a = 0$ al ser $\langle , \rangle$ no degenerada.

□

2.5. Coradicales y filtraciones

Un tema importante en el estudio de las estructuras algebraicas expuestas es el de la *filtración coradical* $\{C_n\}$ (de la coálgebra C). Esta filtración resulta útil como vehículo para argumentos de carácter inductivo. En esta sección se probará el teorema de Heyneman-Radford, que establece que un morfismo de coálgebra es inyectivo si es inyectivo sobre C_1.

En el resto de este capítulo C denota una coálgebra arbitraria. A continuación se presenta el que se conoce como *Teorema fundamental de las coálgebras*, el cual establece que las coálgebras son siempre localmente finitas.

2.31 Teorema (Teorema fundamental de las coálgebras)**.** *Sea C una coálgebra.*

i) *Dado cualquier C-comódulo derecho M y cualquier subconjunto finito $\{m_i\} \subset M$, existe un subcomódulo N de dimensión finita de M tal que $m_i \in N$, para toda i.*

ii) *Dado cualquier subconjunto finito $\{c_i\} \subset C$, existe una subcoálgebra D de dimensión finita de C tal que $c_i \in D$, para toda i.*

Demostración. **i)** Dado que la suma de subcomódulos es nuevamente un subcomódulo, es suficiente probar que cada $m \in M$ se encuentra en un subcomódulo de dimensión finita. Sea $\{c_i\}$ una base para C. Si $\rho : M \to M \otimes C$ es el mapeo con estructura comodular, podemos escribir $\rho(m) = \sum_i w_i \otimes c_i$, donde sólo un número finito de las w_i son cero. Consideremos además $\Delta(c_i) = \sum \alpha_{ijk} c_j \otimes c_k$. Entonces,

$$\sum \rho(w_i) \otimes c_i = (\rho \otimes \mathrm{id})\,\rho(m) = (\mathrm{id} \otimes \Delta)\,\rho(m) = \sum w_i \otimes \alpha_{ijk} c_j \otimes c_k.$$

Comparando los coeficientes de c_k se observa que $\rho(w_k) = \sum w_i \otimes \alpha_{ijk} c_j$. Así, el subespacio N generado por m y las w_i es un subcomódulo.

ii) Al aplicar $i)$ a $M = C$, $\rho = \Delta$, se sigue que $\{c_i\}$ está contenido en un subespacio V de dimensión finita con $\Delta(V) \subseteq V \otimes C$. Sea $\{v_j\}$ una base de V, con $\Delta(v_j) = \sum_i v_i \otimes c_{ij}$. Por la coasociatividad se tiene que $\Delta(c_{ij}) = \sum_k c_{ik} \otimes c_{kj}$. Así, el espacio D generado por $\{v_j\}$ y c_{ij} satisface que $\Delta(D) \subset D \otimes D$. Por construcción, $V \subseteq D$, lo cual prueba $ii)$.

□

2.32 Definición. Se dice que una coálgebra es *simple* si no tiene subcoálgebras propias. Un comódulo es *simple* si no tiene subcomódulos propios.

2.33 Corolario. *Sea C una coálgebra cualquiera. Entonces,*

i) *toda subcoálgebra simple de C es de dimensión finita y*

ii) *todo C-subcomódulo simple es de dimensión finita.*

A continuación se expondrá una caracterización de coálgebras simples en términos de sus duales. Para ello, primero abordaremos algunos aspectos propios del álgebra lineal. Para cualquier espacio vectorial V y subespacio $W \subseteq V$, $W^{\perp} = \{f \in V^* | \langle f, W\rangle = 0\}$; para cualquier subespacio $U \subseteq V^*$, $U^{\perp} = \{v \in V | \langle U, v\rangle = 0\}$. Notemos que $W^{\perp\perp} = W$, pero que puede ocurrir que $U^{\perp\perp}$ contenga propiamente a U si V es de dimensión infinita. Para cualquier $U_1, U_2 \subseteq V^*$, se tiene que

$$(U_1 \otimes U_2)^{\perp} = V \otimes U_2^{\perp} + U_1^{\perp} \otimes V$$

en $V \otimes V$.

Recordemos que, por la Definición 2.6, un subespacio $D \subseteq C$ es un coideal derecho si $\Delta(D) \subseteq D \otimes C$ (o un coideal izquierdo si $\Delta(D) \subseteq C \otimes D$).

2.34 Lema. *Sea C cualquier coálgebra. Entonces,*

i) *D es un coideal derecho (izquierdo) de C si, y sólo si, $D^{\perp}$ es un ideal derecho (izquierdo respectivo) de C^*.*

ii) *si I es un ideal derecho (izquierdo) de C^*, entonces $I^{\perp}$ es un coideal derecho (izquierdo respectivo) de C. El resultado inverso es cierto si C es de dimensión finita.*

En consecuencia, si D es una subcoálgebra de C, entonces

iii) *D es una subcoálgebra simple si, y sólo si, D^* es una álgebra simple de dimensión finita; o si, y sólo si, $D^{\perp}$ es un ideal maximal de C^* de codimensión finita.*

Demostración. **i)** Supongamos que D es un coideal derecho y elijamos $a \in D^{\perp}$, $b \in C^*$. Entonces, $\langle ab, d\rangle = \langle a \otimes b, \Delta(d)\rangle \subseteq \langle a, D\rangle \langle b, C\rangle = 0$, para toda $d \in D$. Por lo tanto, $a, b \in D^{\perp}$, y $D^{\perp}$ es un ideal derecho de C^*. Puesto que $D^{\perp\perp} = D$, el resultado a la inversa se verifica por medio de *ii*).

ii) Sea I un ideal derecho de C^*. Para demostrar que $I^\perp$ es un coideal derecho de C, es suficiente probar que es un C^*-módulo izquierdo bajo $\rightharpoonup$ usando la Definición 2.6. Pero

$$\left\langle I, C^* \rightharpoonup I^\perp \right\rangle = \left\langle IC^*, I^\perp \right\rangle \subseteq \left\langle I, I^\perp \right\rangle = 0.$$

Así, $C^* \rightharpoonup I^\perp \subseteq I^\perp$, y entonces $I^\perp$ es un coideal derecho. A la inversa, cuando C es de dimensión finita, tenemos que $I^{\perp\perp} = I$ y podemos aplicar la primera parte de i).

Las versiones por la izquierda pueden probarse de forma similar usando $\leftharpoonup$.

Para iii), D es una subcoálgebra si, y sólo si, D es un coideal tanto derecho como izquierdo. De este modo, la primera equivalencia se sigue de i), ii) y del Corolario 2.33. La segunda parte se obtiene del hecho de que $D^\perp$ es el kernel del mapeo $\phi : C^* \to D^*$, y entonces $D^* \cong C^*/D^\perp$.

□

2.35 Definición. Sea C una coálgebra.

i) El *coradical* C_0 de C es la suma de todas las subcoálgebras simples de C.

ii) C es *punteada* si toda subcoálgebra simple es de dimensión uno.

iii) C está *conectada* si C_0 es unidimensional.

Necesariamente una subcoálgebra unidimensional es de la forma $\mathbf{k}g$, para $g \in G(C)$. Así, C es punteada si, y sólo si $C_0 \subseteq \mathbf{k}G(C)$. Por otra parte, la suma de subcoálgebras simples es de hecho una suma directa. Se dice que C es *cosemisimple* si C es la suma directa de coálgebras simples. Dicha definición equivale a que $C = C_0$, su coradical.

2.36 Definición. La *filtración coradical* de C es la filtración ascendente

$$C_0 \subseteq C_1 \subset \ldots \subseteq C_j \subseteq C_{j+1} \subseteq \ldots,$$

definida por

$$C_{j+1} = \{x \in C | \Delta(x) \in C_j \otimes C + C \otimes C_0\}.$$

Esto es una *filtración de una coálgebra*:

$$\Delta(C_j) \subseteq \sum_{0 \leq i \leq j} C_i \otimes C_{j-i};$$

y es exhaustiva:

$$C = \bigcup_{n \geq 0} C_n.$$

A continuación la demostración clásica del Teorema de Heyneman-Radford.

2.37 Teorema (Teorema de Heyneman-Radford)**.** *Sean C y D coálgebras y $f : C \to D$ un morfismo de coálgebras tales que $f|_{C_1}$ es inyectiva. Entonces f es inyectiva.*

La demostración de este hecho exige algunos lemas.

2.38 Lema. *Sea C una álgebra conectada, con $G(C) = \{1\}$. Entonces*

i) *$C_1 = \mathbf{k}1 \oplus P(C)$, donde $P(C)$ es el conjunto de elementos primitivos de C.*

ii) *Para cualquier $n \geq 1$ y $c \in C_n$, $\Delta(c) = c \otimes 1 + 1 \otimes c + y$, donde $y \in C_{n-1} \otimes C_{n-1}$.*

Demostración. ii) Por la Definición 2.36, $\Delta(c) \in C_n \otimes C_0 + C_0 \otimes C_n \sum_{i=1}^{n-1} c_i \otimes C_{n-i}$. Dado que $C_0 = \mathbf{k}1$, podemos escribir $\Delta(c) = a \otimes 1 + 1 + \otimes b + w$, para $w \in C_{n-1} \otimes C_{n-1}$. Ahora $c = (\mathrm{id} \otimes \epsilon)\Delta(c) = a + \epsilon(b)1 + (\mathrm{id} \otimes \epsilon) \in a + C_0 + C_{n-1}$; y así, $a - c = c' \in C_{n-1}$. De manera similar, $b - c = c'' \in C_{n-1}$. Se sigue que $\Delta(c) = c \otimes 1 + 1 \otimes c + y$, para $y = w + c' \otimes 1 + 1 \otimes c'' \in C_{n-1} \otimes C_{n-1}$.

Para $i)$, elegiremos $c \in C_1$. Entonces, $\Delta(c) = c \otimes 1 + 1 \otimes c + \alpha(1 \otimes 1)$, $\alpha \in \mathbf{k}$, por $ii)$. Usando $c = (\mathrm{id} \otimes \epsilon)\Delta(c)$ se tiene que $\alpha = -\epsilon(c)$; entonces se sigue que $c - \epsilon(c)1 \in P(C)$. Por lo tanto, $C_1 = \mathbf{k}l + P(C)$. La suma es directa ya que $\epsilon(P(C)) = 0$. □

2.39 Lema. *Si C es conectada y $f : C \to D$ es un mapeo de coálgebras tal que $f|_{P(C)}$ es inyectiva, entonces f es inyectiva.*

Demostración. Se mostrará que $f|C_n$ es inyectiva para toda $n \geq 0$. Puesto que f es un mapeo de coálgebras, $\epsilon(f(1)) = \epsilon(1) = 1$ y entonces $f(1) \neq 0$. También, $\epsilon(f(P(C))) = 0$ y así $f(\mathbf{k}1) + f(P(C))$ es una suma directa. Del Lema 2.38, $i)$, se sigue que $f|_{C_1}$ es inyectiva.

Ahora, asumamos que $f|_{C_n}$ es inyectiva y elijamos $x \in C_{n+1}$. Por el Lema 2.38, $ii)$, $\Delta(x) = x \otimes 1 + 1 + \otimes x + y$, para $y \in C_n \otimes C_n$. Así, $\Delta(f(x)) = (f \otimes f)\Delta(x) = f(x) \otimes f(1) + f(1) \otimes f(x) + (f \otimes f)(y)$. Si $x \in \ker f$, entonces $(f \otimes f)y = 0$. Pero, $f \otimes f$ es inyectiva en $C_n \otimes C_n$, y entonces $y = 0$. Pero entonces $x \in P(C) \subset C_1$ y sabemos que f es inyectiva en C_1; por lo tanto, $x = 0$ y f es inyectiva. □

2.40 Lema. *Sea C cualquier coálgebra y $\{A_n\}$ una filtración de coálgebra de C. Entonces, $C_0 \subseteq A_0$.*

Demostración. Es suficiente mostrar que si D es cualquier subcoálgebra distinta de cero de C, entonces $D \cap A_0 \neq 0$. Al ser $\cup_{n\geq 0} A_n = C$, podemos elegir una n minimal tal que $D \cap A_n \neq 0$; tomemos $n = 0$. Escojamos $0 \neq d \in D \cap A_n$. Entonces $i)$ $\Delta(d) \in \sum_{i=0}^{n} A_i \otimes A_{n-i}$ y $ii)$ $\Delta(d) \in D \otimes D$. Si $\Delta(d) \in C \otimes A_0$, entonces $d = (\epsilon \otimes \mathrm{id})\Delta(d) \in A_0$. Si no, se elige $f \in C^*$ con $f \in A_0^{\perp}$ y $0 \neq \langle \mathrm{id} \otimes f, \Delta(d) \rangle = \bar{d}$. Por $i)$, $\bar{d} \in A_{n-1}$, y por $ii)$ $\bar{d} \in D$. Por lo tanto, $\bar{d} \in D \cap A_{n-1}$ es una contradicción. En consecuencia $D \cap A_0 \neq 0$. □

2.41 Corolario. *Si $f : C \to D$ es un mapeo de coálgebras suprayectivo, entonces $f(C_0) \supset D_0$. Por lo tanto, si C es punteada, $f(C_0) = D_0$ y D es punteada.*

Demostración. Sea $A_n = f(C_n)$, con $n \geq 0$. Entonces, $\{A_n\}$ es una filtración coradical de D. Por el Lema 2.40, $D_0 \subset A_0 = f(C_0)$. □

2.42 Lema. *Sea $f : C \to D$ un mapeo de coálgebras suprayectivo y sean W_1, W_2 subespacios de C tales que* $\ker f \subseteq W_1 \cap W_2$. *Entonces*

$$f(W_1 \wedge W_2) = f(W_1) \wedge f(W_2).$$

Demostración. Definamos $f_i : C/W_i \to D/f(W_i)$, $i = 1, 2$ como los mapeos inducidos de f en los cocientes. Entonces, el $\ker f \subseteq W_i$ implica que f_1, f_2 y entonces $f_1 \otimes f_2$ son biyectivos. Ahora, definamos a α y β como las composiciones

$$\begin{aligned} \alpha :& C \to C \otimes C \to C/W_1 \otimes C/W_2 = \tilde{C} \\ \beta :& D \to D \otimes D \to D/f(W_1) \otimes D/f(W_2) = \tilde{D}. \end{aligned}$$

De la definición de $\wedge$, $\ker \alpha = W_1 \wedge W_2$ y $\ker \beta = f(W_1) \wedge f(W_2)$. Debe mostrarse que $\ker \beta = f(\ker \alpha)$. Dado que $f_1 \otimes f_2$ es biyectiva y f es suprayectiva, lo anterior se obtiene mediante el siguiente diagrama conmutativo:

$$\begin{array}{ccc} C & \xrightarrow{f} & D \\ {\scriptstyle \alpha}\downarrow & & \downarrow{\scriptstyle \beta} \\ \tilde{C} & \xrightarrow{f_1 \otimes f_2} & \tilde{D} \end{array}$$

□

2.43 Definición. Sea C cualquier coálgebra, y sea $C^+ = \ker \epsilon$. Entonces la coálgebra conectada asociada de C es $R = R(C) = C/C_0^+$.

Debe probarse que $R(C)$ es de hecho conectada. Sea $\pi : C \to R(C)$ el mapeo cociente canónico.

2.44 Lema. *Para toda $n \geq 0$, $R(C)_n = \pi(C_n)$; en particular $R(C)$ es conectada.*

Demostración. Escribamos $R = R(C)$ por simplicidad. Ahora, $\pi(C_0) \supseteq R_0$, por el Corolario 2.41; sin embargo, $\pi(C_0) = C_0/C_0^+$ es unidimensional. Así, $\pi(C_0) = R_0$ y R es conectada. Ahora se aplicará el Lema 2.42 con $f = \pi$; al ser $\ker \pi = C_0^+ \subseteq C_0^+ \subset C_0 \cup C_{n-1}$ para toda $n \geq 1$, se sigue que $\pi(C_0 \wedge C_{n-1}) = \pi(C_0) \wedge \pi(C_{n-1})$ para toda $n \geq 1$. Por inducción, $\pi(C_{n-1}) = R_{n-1}$; por lo tanto, $\pi(C_n) = R_0 \wedge R_{n-1} = R_n$. □

Ahora se tienen los elementos necesarios para la demostración formal del Teorema de Heyneman-Radford, pues es suficiente con probar que si N es un coideal en C tal que $N \cap C_1^+ = 0$, donde $C_1^+ = C_1 \cap \ker \epsilon$, entonces $N = 0$. Si se aplica esto con $N = \ker f$, entonces $N \cap C_1^+ = 0$ implica $N = 0$.

Sea R la coálgebra conectada asociada y $\pi : C \to R$ el mapeo cociente, como arriba, y asumamos que $N \cap C_1^+ = 0$. Pretendemos que $\pi(N) \cap R_1^* = 0$. Para ello es suficiente mostrar que $\pi(N) \cap \pi\left(C_1^+\right) = 0$ ya que $\pi\left(C_1^+\right) = R_1^+$ por el Lema 2.44. Elijamos $r \in \pi(N) \cap \pi(C_1+)$; escribamos $r = \pi(n) = \pi(c)$, por $n \in N$, $c \in C_1^+$. Entonces, $n - c \in \ker \pi = C_0^+ \subseteq C_1^+$, y entonces $n \in N \cap C_1^+ = 0$. Por lo tanto, $r = \pi(n) = 0$, lo cual prueba el hecho deseado.

Ahora consideremos $g : R \to R/\pi(N) = \pi(C)/\pi(N) = \pi(C/N)$. R es conectada y g es inyectiva en R_1^+ puesto que $\pi(N) \cap R_1^+ = 0$. Por lo tanto, por el Lema 2.39, g es inyectiva en R. Así, $\ker g = \pi(N) = 0$. Entonces, $N \subseteq \ker \pi = C_0^+ \subseteq C_1^+$, y por lo tanto, $N = N \cap C_1^+ = 0$.

Capítulo 3

Grupos cuánticos

El desarrollo de la teoría de los grupos cuánticos revivió el interés en las álgebras de Hopf. A principios de 1980, varios matemáticos comenzaron a trabajar en estructuras a las que hoy en día llamamos *grupos cuánticos*. Los primeros ejemplos de grupos cuánticos fueron deformaciones particulares de álgebras universales envolventes de álgebras de Lie simples. A mediados de esta misma década, Drinfeld mostró que el marco teórico propicio para el estudio de los grupos cuánticos era el de las álgebras de Hopf, según consta en [18]. De manera que, desde entonces, el mundo de las álgebras de Hopf se expandió y los hallazgos sobre grupos cuánticos le dieron nuevos matices a la teoría clásica.

Aunque no hay a la fecha un consenso en la definición precisa de lo que es un grupo cuántico, en general, puede entenderse como un tipo especial de álgebra de Hopf no conmutativa y nococonmutativa. Se obtienen dichas álgebras de Hopf al deformar el producto o el coproducto de una álgebra de Hopf conmutativa o coconmutativa. Puesto que el resultado final de dicha deformación no es conmutativo, no puede asociarse propiamente a un grupo o ser una función de álgebra. De manera similar, al no ser coconmutativo, tampoco es de forma alguna el álgebra envolvente de una álgebra de Lie. Sin embargo, podemos considerarle como si fuera la función de álgebra del álgebra universal envolvente de algún grupo o álgebra de Lie ficticios y de ahí que se emplee el término "grupo cuántico".

En este capítulo se hará una introducción al tema bajo el enfoque propuesto por Kharchenko [37], en donde la noción de álgebra universal envolvente cuántica para cualquier álgebra de Lie es definida a través de generadores y relaciones basadas en el concepto

de operaciones cuánticas de Lie. Estos resultados serán de utilidad más adelante para el estudio del rango combinatorio de un grupo cuántico particular.

3.1. Álgebras envolventes cuánticas

En la práctica, los estudiosos de los grupos de Lie y de las álgebras de Lie, emplean letras góticas minúsculas para denotar las álgebras de Lie, particularmente $\mathfrak{g}$ para denotar una típica álgebra de Lie. No se sabe con certeza de dónde proviene esta práctica, pero es posible que ello se atribuya al alemán Hermann Weyl, quien fue uno de los principales desarrolladores de la teoría de Lie (y de muchos otros temas matemáticos) de mediados del siglo XX.

3.1 Definición. Sea $\mathbf{k}$ un campo. El *álgebra de Lie* sobre $\mathbf{k}$ es un espacio vectorial $\mathfrak{g}$ sobre $\mathbf{k}$ con el mapeo $[\ ,\ ] : \mathfrak{g} \otimes \mathfrak{g} \to \mathfrak{g}$ que satisface:

i) $[x, x] = 0$, para toda $x \in \mathfrak{g}$,

ii) $[x, [y, z]] + [z, [x, y]] + [y, [z, x]] = 0$, para todas $x, y, z \in \mathfrak{g}$.

La multiplicación en el álgebra de Lie $\mathfrak{g}$ se llama *corchete* de Lie. La primera relación de la definición es conocida como la *relación simétrica torcida* y es equivalente a $[x, y] = -[y, x]$ para todas $x, y \in \mathfrak{g}$, siempre que la característica de $\mathbf{k}$ sea distinta de 2. Cualquier producto algebraico que satisface la primera condición se dice que es *anticonmutativo*.

La segunda relación es la *identidad de Jacobi*. Una álgebra de Lie $\mathfrak{g}$ sobre $\mathbf{k}$ es de *dimensión finita* si es de dimensión finita como espacio vectorial sobre $\mathbf{k}$, y es *compleja* si $\mathbf{k} = \mathbb{C}$.

Una variable es llamada *variable cuántica* si un elemento g_x de un grupo abeliano G y un caracter $\chi^x \in G^*$ está asociado a ella. Los parámetros g_x y χ^x asociados a una variable cuántica dicen que un elemento a en una álgebra de Hopf H puede considerarse como un valor de esta variable cuántica sólo si a es primitiva torcida semi-invariante con los mismos parámetros, esto es

$$\Delta\left(a \otimes 1 + g_x \otimes a\right), \qquad g^{-1} a g = \chi^x\left(g\right) a, \qquad g \in G,$$

donde supondremos que los elementos de G tienen alguna interpretación en H como elementos de tipo grupo.

Un polinomio no conmutativo en variables cuánticas se llama *operación cuántica de Lie* si todos sus valores en todas las álgebras de Hopf son primitivos torcidos para todos los valores de las variables cuánticas.

Sean $x_1, \ldots, x_n$ un conjunto de variables cuánticas. Para cada palabra u en $x_1, \ldots, x_n$ denotaremos por g_u a un elemento de G que aparece de u al reemplazar a toda g_i con g_{x_i}. De igual manera, denotemos por χ^u al caracter que aparece en u al reemplazar a todas las x_i por χ^{x_i}. Así, en el álgebra libre $\mathbf{k}\langle x_1, \ldots, x_n\rangle$ se define una clasificación por medio del grupo $G \times G^*$. Para cada par de elementos homogéneos u y v fijaremos la siguiente notación $p_{uv} = \chi^u(g_v) = p(u, v)$.

Definiremos una acción de G en $\mathbf{k}\langle x_1, \ldots, x_n\rangle$ por medio de $g^{-1}ug = \chi^u(g)\, u$ donde u es un monomio arbitrario en $x_1, \ldots, x_n$. El álgebra de grupo torcida $G\langle X\rangle = \mathbf{k}\langle x_1, \ldots, x_n\rangle * G$ tiene una estructura natural de álgebra de Hopf con el coproducto

$$\Delta(x_i) = x_i \otimes 1 + g_{x_i} \otimes x_i, \quad 1 \leq i \leq 1, \quad \Delta(g \otimes g), \quad g \in G.$$

Así, $x_i = x_i \in G\langle X\rangle$ son valores correctos de las variables cuánticas. Por este medio las operaciones cuánticas de Lie pueden identificarse con polinomios torcidos primitivos en $G\langle X\rangle$. Es importante destacar que el álgebra de Hopf $G\langle X\rangle$ es el *álgebra envolvente libre* para el conjunto X de variables cuánticas (véase [34, Sección 3] bajo la notación $H\langle X\rangle$).

El álgebra libre $\mathbf{k}\langle x_1, \ldots, x_n\rangle$ tiene estructura de álgebra de Hopf trenzada biclasificada. Sea $\mathcal{H}$ una álgebra asociativa clasificada por el grupo $G \times G^*$:

$$\mathcal{H} = \sum_{g \in G, \chi \in G^*} \oplus \mathcal{H}_g^{\chi}.$$

Definamos la multiplicación del producto tensorial $\mathcal{H} \otimes \mathcal{H}$ de espacios lineales estableciendo

$$(a \otimes b) \cdot (c \otimes d) = \left(\chi^c(g_b)\right)^{-1} (ac \otimes bd).$$

El resultado es una álgebra asociativa, denotada por $\mathcal{H} \underline{\otimes} \mathcal{H}$. Ahora, si en la definición de álgebra de Hopf cambiamos el símbolo $\otimes$ por $\underline{\otimes}$ y asumimos que el coproducto Δ^b,

la counidad ϵ^b y la antípoda S^b son homogéneos, llegamos a la definición de *álgebra de Hopf trenzada bicategorizada*. En otras palabras una álgebra de Hopf biclasificada es una álgebra de Hopf clasificada por $G \times G^*$ en una categoría trenzada en la que el trenzado está conectado con la clasificación por la fórmula $c\left(u \otimes v\right) = \left(\chi^v\left(g_u\right)\right)^{-1}\left(v \otimes u\right)$.

La operación cuántica de Lie puede definirse de forma equivalente como un polinomio homogéneo de $G \times 1$ que tiene sólo valores primitivos en todas las álgebras de Hopf trenzadas biclasificadas dado que el valor correcto de la variable cuántica $x = x_g^\chi$ es primitivo y homogéneo, esto es $a \in \mathcal{H}_g^\chi$, $\Delta^b\left(a\right) = a \underline{\otimes} 1 + 1 \underline{\otimes} a$. La discusión detallada de la noción de operación cuántica de Lie, así como varios ejemplos pueden encontrarse en [34, Secciones 1–4].

Recordemos que la *constitución* de una palabra u es una secuencia de enteros no negativos. $(m_1, m_2, \ldots, m_n)$ tal que u es de grado m_1 en x_1, $\deg_1\left(u\right) = m_1$; de grado m_2 en x_2, $\deg_2\left(u\right) = m_2$; y así sucesivamente ([65, Definición 3]). Dado que el grupo G es abeliano, todo polinomio de constitución homogénea es homogéneo con respecto de la clasificación. Definamos un conmutador bilineal torcido en el conjunto de polinomios no conmutativos homogéneos clasificados por la fórmula

$$[u, v] = uv - p_{uv} vu. \tag{3.1}$$

Estos corchetes satisfacen las siguientes identidades de Jacobi y diferenciales torcidas:

$$[[u, v], w] = [u, [v, w]] + p_{wv}^{-1}\left[[u, w], v\right] + \left(p_{vw} - p_{wv}^{-1}\right)[v, w] \cdot v; \tag{3.2}$$

$$[[u, v], w] = [u, [v, w]] + p_{vw}\left[[u, w], v\right] + p_{uv}\left(p_{vw} p_{wv} - 1\right) v \cdot [u, w]; \tag{3.3}$$

$$[u, v \cdot w] = [u, v] \cdot w + p_{uv} v \cdot [u, w]; \quad [u \cdot v, w] = p_{vw}\,[u, w] \cdot v + u \cdot [v, w], \tag{3.4}$$

donde por el punto denotamos la multiplicación habitual. Las siguientes identidades restringidas condicionales también son válidas:

$$[u, v^n] = [\ldots [[u, v], v] \ldots, v]; \quad [v^n, u] = [v, [\ldots, [v, u] \ldots]], \tag{3.5}$$

dado que p_{uv} es una raíz t-ésima de unidad primitiva y $n = t$ o $n = tl^k$ en el caso de que la característica sea $l > 0$.

Supongamos que una álgebra de Lie $\mathfrak{g}$ está definida por los generadores $x_1, \ldots, x_n$ y las relaciones $f_i = 0$. Convirtamos los generadores en variables cuánticas. Para ello les asociaremos elementos de $G \times G^*$ de manera arbitraria. Sea $P = \|p_{ij}\|$, $p_{ij} = \chi^{x_i}\left(g_{x_j}\right)$ la *matriz cuantificadora*.

3.2 Definición. Una *álgebra envolvente cuántica trenzada* de $\mathfrak{g}$ es una álgebra de Hopf trenzada biclasificada $U_P^b(\mathfrak{g})$ definida por las variables $x_1, \ldots, x_n$ y las relaciones $f_i = 0$, donde la operación de Lie es reemplazada con (3.1), dado que de esta forma las f_i son convertidas a las operaciones cuánticas de Lie, f_i^*. El coproducto y la clasificación están dados por

$$\Delta^b(x_i) = x_i \underline{\otimes} 1 + 1 \underline{\otimes} x_i, \tag{3.6}$$

$$(x_i \underline{\otimes} x_j) \cdot (x_k \underline{\otimes} x_m) = \left(\chi^{x_k}\left(g_{x_j}\right)\right)^{-1} x_i x_k \underline{\otimes} x_j x_m. \tag{3.7}$$

3.3 Definición. Una *cuantificación simple* de $U(\mathfrak{g})$ o una *álgebra universal envolvente cuántica* de $\mathfrak{g}$ es una álgebra $U_P(\mathfrak{g})$ que es isomórfica al álgebra de grupo torcida

$$U_P(\mathfrak{g}) = U_P^b(\mathfrak{g}) * G, \tag{3.8}$$

donde la acción de grupo y el coproducto están definidos por

$$g^{-1} x_i g = \chi^{x_i}(g)\, x_i, \quad \Delta(x_i) = x_i \otimes 1 + g_{x_i} \otimes x_i, \quad \Delta(g) = g \otimes g. \tag{3.9}$$

3.4 Definición. Una *cuantificación con constantes* es una cuantificación simple donde adicionalmente algunos generadores x_i asociados al caracter trivial son reemplazados por las constantes $\alpha_i(1 - g_{x_i})$.

Las fórmulas (3.9) y (3.6) definen correctamente el coproducto, pues por la definición de la operación cuántica de Lie $\Delta(f_i^*) = f_i^* \otimes 1 + g_i \otimes f_i^*$ en el caso de álgebras de Hopf ordinarias y $\Delta^b(f_i^*) = f_i^* \underline{\otimes} 1 + 1 \underline{\otimes} f_i^*$ en el caso trenzado.

Es importante notar que las cuantificaciones definidas dependen esencialmente de la representación combinatoria del álgebra de Lie. Por ejemplo, una relación adicional $[x_1, x_1] = 0$ no cambia el álgebra de Lie. Al mismo tiempo, si $\chi^{x_1}(g_1) = -1$ entonces esta relación admite la cuantificación y conduce a una relación no trivial del álgebra cuántica envolvente, $2x_1^2 = 0$.

3.5 Ejemplo. Supongamos que el álgebra de Lie está definida por un sistema de relaciones cuya constitución es homogénea. Si los caracteres χ^i son tales que $p_{ij}p_{ji} = 1$ para todas i, j entonces el conmutador torcido es él mismo una operación cuántica. Por lo tanto, al reemplazar la operación de Lie, todas las operaciones se vuelven operaciones cuánticas también. Esto significa que el álgebra envolvente trenzada es el álgebra universal envolvente $U\left(\mathfrak{g}^{\mathrm{col}}\right)$ de la súper álgebra de Lie coloreada que está definida por las mismas relaciones que definen al álgebra de Lie. La cuantificación simple aparece como el biproducto de Radford $U\left(\mathfrak{g}^{\mathrm{col}}\right) * \mathbf{k}\left[G\right]$ o, de manera equivalente, como el álgebra universal G-envolvente de la súper álgebra de Lie coloreada $\mathfrak{g}^{\mathrm{col}}$ (véase [59] o [34, Ejemplo 1.9]).

3.6 Ejemplo. Supongamos que el álgebra de Lie $\mathfrak{g}$ está definida por los generadores $x_1, \ldots, x_n$ y el sistema de relaciones nil

$$x_j \left(\mathrm{ad} \quad x_i\right)^{n_{ij}} = 0, \quad 1 \leq i \neq j \leq n. \tag{3.10}$$

Frecuentemente, en lugar de la matriz de grados (sin la diagonal principal), $\|n_{ij}\|$, se considera a la matriz $A = \|a_{ij}\|$, $a_{ij} = 1 - n_{ij}$. La gráfica de Coxeter $\Gamma\left(A\right)$ está asociada a toda matriz de ese tipo. Esta gráfica tiene los vértices $1, \ldots, n$, donde el vértice i está conectado por medio de $a_{ij}a_{ji}$ aristas al vértice j.

Si $a_{ij} = 0$, entonces la relación $x_j \mathrm{ad}\ x_i = 0$ está en la lista (3.10), y la relación $x_i \left(\mathrm{ad}\ x_j\right)^{n_{ji}} = 0$ es una consecuencia de ello. El conmutador torcido $[x_j, x_i]$ es una operación cuántica de Lie si y sólo si $p_{ij}p_{ji} = 1$. Bajo esta condición tenemos que $[x_i, x_j] = -p_{ij}\left[x_j, x_i\right]$. Por lo tanto, ambos en el álgebra de Lie y en su cuantificación pueden reemplazar la relación $x_i \left(\mathrm{ad}\ x_j\right)^{n_{ij}} = 0$ con $x_i \mathrm{ad}\ x_j = 0$.

En otras palabras, sin pérdida de generalidad, podemos suponer que $a_{ij}0 \longleftrightarrow a_{ij} = 0$. Por el teorema de Gabber-Kac [19], tenemos que el álgebra $\mathfrak{g}$ es el componente positivo homogéneo $\mathfrak{g}_1^+$ del álgebra de Kac-Moody $\mathfrak{g}_1$.

El siguiente teorema describe las condiciones para un polinomio homogéneo en dos variables que es lineal a una de ellas para ser una operación cuántica.

3.7 Teorema. *Para variables cuánticas x_1 y x_2, existe una operación cuántica de Lie W lineal, distinta de cero, en x_1 de grado n en x_2 si y sólo si $p_{12}p_{21} = p_{22}^{1-n}$, o bien, p_{22} es una raíz m-ésima primitiva de unidad, $m|n$, y $p_{12}^m p_{21}^m = 1$. Si una de esas condiciones se satisface, entonces todas las operaciones tienen la forma $W = \alpha\left[\ldots\left[\left[x_1 x_2\right] x_2\right]\ldots x_2\right]$, $\alpha \in \mathbf{k}$, donde los corchetes están definidos como en* (3.1).

Demostración. Se sigue del Teorema 6.1 [34] y la identidad condicional (3.5). □

De este teorema, se desprende el siguiente corolario:

3.8 Corolario. *Si n_{ij} es un número simple o una unidad y en el primer caso p_{ii} no es una raíz n_{ij}-ésima primitiva de unidad, entonces la relación* (3.10) *admite una cuantificación si y sólo si $p_{ij}p_{ji} = p_{ii}^{a_{ij}}$.*

El Teorema 3.7 brinda restricciones no esenciales en los parámetros fuera de la diagonal principal, p_{ij}: si la matriz P define de forma correcta una cuantificación de (3.10), entonces para todo conjunto $Z = \{z_{ij} | z_{ij}z_{ji} = z_{ii} = 1\}$ la siguiente matriz también lo hace:

$$p_Z = \{p_{ij}z_{ij} | p_{ij} \in P, z_{ij} \in Z\}. \tag{3.11}$$

3.9 Ejemplo. Sea G generada libremente por $g_1, \ldots, g_n$ y A una matriz de Cartan generalizada hecha simétrica por $d_1, \ldots, d_n$, mientras los caracteres están definidos por $p_{ij} = q^{-d_i a_{ij}}$. En este caso la cuantificación simple de $\mathfrak{g}$ definida por (3.10) es el componente positivo del álgebra envolvente de Drinfeld-Jimbo junto con los elementos de tipo grupo $U_P(\mathfrak{g}) = U_q^+(\mathfrak{g}) * G$. Por medio de una deformación arbitraria (3.11) puede definirse una forma coloreada de $U_q^+(\mathfrak{g}) * G$.

El álgebra envolvente trenzada es igual con $U_q^+(\mathfrak{g})$ donde el coproducto y el trenzado están definidos por (3.6) y (3.7) con coeficientes $q^{d_k a_{kj}}$. La fórmula (3.11) define correctamente su forma coloreada también.

3.10 Ejemplo. En el ejemplo anterior completamos el conjunto de variables cuánticas con las nuevas $x_1^-, \ldots, x_n^-$, $z_1, \ldots, z_n$ tales que

$$\chi^{x^-} = (\chi^x) - 1,\ g_{x^-} = g_x,\ \chi^{z_i} = \mathrm{id},\ g_{z_i} = g_i^2, \tag{3.12}$$

entonces por el Teorema 3.7, las relaciones de Gaber-Kac (3.1), (3.2) de [19, Teorema 2], y $[e_i, f_j] = \delta_{ij}h_i$ bajo la identificación $e_i = x_i$, $f_i = x_i^-$, $h_i = z_i$ admiten la cuantificación con constantes $z_i = \epsilon_i(1 - g_i^2)$. Informalmente podemos considerar la cuantificación obtenida como una del álgebra de Kac-Moody identificada por g_i con q^{h_i}, donde el resto de las relaciones del álgebra de Kac-Moody, $[h_i, e_j] = a_{ij}e_i$, $[h_i, f_j] = -a_{ij}f_j$, está cuantificada en cuanto a la acción sobre G: $g_j^{-1}x_i^{\pm}g_j = p^{\mp d_{ij}a_{ij}}x_i^{\pm}$. Esta cuantificación coincide con la de Drinfeld-Jimbo bajo una elección de x_i, x_i^-, y ϵ_i dependiendo de la definición particular de $U_q(\mathfrak{g})$:

$$
\begin{aligned}
x_i = E_i,\ g_i = K_i,\ x_i^- = F_i K_i,\ p_{ij} = v^{-d_i a_{ij}},\ \epsilon_i = \left(v^{-d_i} - v^{d_i}\right)^{-1};\\
x_i = E_i,\ g_i = \tilde{K}_i,\ x_i^- = F_i \tilde{K}_i,\ p_{i\mu} = v^{\langle -\mu, i' \rangle},\ \epsilon_i = \left(v_i^{-1} - v_i\right)^{-1};\\
\Delta_+ : x_i = e_i,\ g_i = t_i,\ x_i^- = t_i f_i,\ p_{ij} = q_j^{-\langle h_j, \alpha_i \rangle},\ \epsilon_i = \left(q_i^{-1} - q_i^3\right)^{-1};\\
\Delta_- : x_i = f_i,\ g_i = t_i,\ x_i^- = e_i t_i,\ p_{ij} = q_j^{\langle h_j, \alpha_i \rangle},\ \epsilon_i = \left(q_i^{-1} - q_i\right)^{-1};\\
x_i = E_i K_i,\ g_i = K_i^2,\ x_i^- = F_i K_i,\ p_{ij} = q^{-2 d_i a_{ij}},\ \epsilon_i = \left(1 - q^{4 d_i}\right)^{-1}.
\end{aligned}
$$

Por (3.12) los corchetes $\left[x_i, x_j^-\right]$ son las operaciones cuánticas de Lie sólo si $p_{ij} = p_{ji}$. Así, en este caso, el coloreado definido por (3.11) puede ser sólo blanco o negro, $z_{ij} = \pm 1$.

3.2. Rango combinatorio

Una álgebra de Hopf se llama *caracter* si el grupo G de todos los elementos de tipo grupo son conmutativos y H es generada por elementos primitivos torcidos semiinvariantes a_i:

$$\Delta(a_i) = a_i \otimes 1 + g_{a_i} \otimes a_i,\ g^{-1} a_i g = \chi^{a_i}(g)\, a_i,\ g \in G. \tag{3.13}$$

Por las definiciones de la sección previa, las álgebras cuánticas envolventes (con o sin constantes) son álgebras de Hopf caracter. En esta sección, por medio de la noción de rango combinatorio, identificaremos las álgebras cuánticas envolventes en la clase de las álgebras de Hopf caracter.

Sea H una álgebra de Hopf caracter generada por semiinvariantes primitivos torcidos $a_1, \ldots, a_n$. Asociemos una variable cuántica x_i con los parámetros (χ^{a_i}, g_{a_i}) a a_i. Denotemos por $G\langle X \rangle$ el álgebra envolvente libre definida por las variables cuánticas $x_1, \ldots, x_n$. El mapeo $x_i \to a_i$ tiene una extensión a un homomorfismo de álgebras de Hopf $\phi : G\langle X \rangle \to H$. Denotemos con I el kernel de dicho homomorfismo. Si $I \neq 0$ entonces, por el Teorema de Heyneman-Radford, el ideal de Hopf I tiene un elemento primitivo torcido distinto de cero. Sea I_1 el ideal generado por todos los elementos primitivos torcidos de I. I_1 es también un ideal de Hopf. Ahora, consideremos el ideal de Hopf I/I_1 del álgebra de Hopf cociente $G\langle X \rangle / I_1$. Este ideal también tiene elementos primitivos torcidos distintos de cero, dado que $I_1 \neq I$. Denotemos por I_2/I_1 al ideal generado por todos los elementos primitivos torcidos de I/I_1, donde I_2 es su preimagen con respecto de la proyección $G\langle X \rangle \to G\langle X \rangle / I_1$. Si continuamos el proceso encontraremos una cadena estrictamente creciente, finita o infinita, de ideales de Hopf de

$G\langle X\rangle$:

$$0 = I_0 \subset I_1 \subset I_2 \subset \ldots \subset I_n \subset \ldots, \quad \bigcup_\alpha I_\alpha = I. \tag{3.14}$$

3.11 Definición. La longitud de (3.14) se llama *rango combinatorio* de H.

Por definición, el rango combinatorio de cualquier álgebra cuántica envolvente (con constantes) es iguala 1. En el caso de que la característica sea cero, la afirmación es válida también a la inversa.

3.12 Teorema. *Cada álgebra de Hopf caracter de rango combinatorio 1 sobre un campo de característica cero es isomórfico al álgebra cuántica envolvente con constantes de una álgebra de Lie.*

Demostración. Por definición, I está generado por elementos primitivos torcidos. Dichos elementos, como polinomios no conmutativos, son las operaciones cuánticas de Lie. Consideremos a uno de ellos, digamos, f. Descompongamos a f en la suma de componentes homogéneos $f = \sum f_i$. Todos los componentes positivos perteneces a $\mathbf{k}\langle X\rangle$ y son las operaciones cuánticas de Lie, mientras que el elemento constante tiene la forma $\alpha(1-g)$, $g \in G$ (véase [34, Sec. 3 y Prop. 3.3]). Si $\alpha \neq 0$, entonces introduciremos una nueva variable cuántica z_f con parámetros (id, g). Cada f_i tiene una representación por medio de conmutadores torcidos. De hecho, por [34, Teorema 7.5] la linealización completa f_i^{lin} de f_i tiene la representación requerida. Por medio de la identificación de variables en una forma adecuada en f_i^{lin} obtenemos la representación requerida para f_i multiplicada por un número natural, $m_i f_i = f_i^{[\ ]}$.

Ahora, consideremos el álgebra de Lie $\mathfrak{g}$ definida por los generadores x_i, z_f y las relaciones $\sum m_i^{-1} f_i^{[\ ]} + z_f = 0$, con la multiplicación de Lie en lugar del conmutador torcido. Entonces H es la cuantificación con constantes de $\mathfrak{g}$. □

De igual manera puede introducirse la noción de rango combinatorio del álgebra de Hopf trenzada biclasificada. En este caso, todas las álgebras cuánticas envolventes son de rango 1, y todas las álgebras trenzadas biclasificadas de rango 1 son la cuantificación trenzada de alguna álgebra de Lie.

Ahora podemos definir la cuantificación de un *rango arbitrario*. Para ello, en las definiciones de la sección anterior es necesario cambiar el requerimiento de que todas las f_i^* sean operaciones cuánticas de Lie por la siguiente condición.

El conjunto F se expresa como la unión $F = \cup_{j=1}^{n} F_j$ tal que F_1^* consiste en las operaciones cuánticas de Lie; el conjunto F_2^* consiste en elementos primitivos torcidos de $G\langle X||F_1^*\rangle$; el conjunto F_3^* consiste en elementos primitivos torcidos de $G\langle X||F_1^*, F_2^*\rangle$, y así sucesivamente.

Las álgebras cuánticas envolventes de rango arbitrario son también álgebras de Hopf caracter. A la inversa, si una álgebra de Hopf caracter H es homogénea y el campo base tiene característica cero, entonces H es una cuantificación de algún rango de una álgebra de Lie adecuada (véase [36]). No es claro si existen álgebras de Hopf caracter, o álgebras de Hopf trenzadas bicategorizadas, de rango combinatorio infinito; pero $\cup_{n=1}^{\infty} I_n = I$. También es posible mostrar que F_1 siempre contiene todas las relaciones de constitución mínima en F. Por ejemplo, cada una de las formas (3.10) es de constitución mínima en (3.10). Por lo tanto, la cuantificación de un rango arbitrario con la identificación $g_i = \exp(h_i)$ para cualquier álgebra de Kac-Moody $\mathfrak{g}$ (generalizada), o su componente nilpotente $\mathfrak{g}^+$, es siempre una cuantificación en el sentido expuesto en la sección anterior.

3.3. Generadores Poincarè-Birkhoff-Witt

El siguiente resultado produce una base Poincarè-Birkhoff-Witt (PBW) para las álgebras cuánticas envolventes.

3.13 Teorema. *Toda álgebra de Hopf caracter H tiene un conjunto linealmente ordenado de elementos de constitución homogénea $U = \{u_i | i \in I\}$ tales que el conjunto de todos los productos $g u_1^{n_1} u_2^{n_2} \dots u_m^{n_m}$, donde $g \in G$, $u_1 < u_2 < \dots < u_m$, $0 \leq n_i < h(i)$ forma una base de H. Aquí, si $p_{ii} \overset{\text{def}}{=} p_{u_i} p_{u_i}$, no es una raíz de unidad entonces $h(i) = \infty$; si $p_{ii} = 1$, entonces $h(i) = \infty$ o $h(i) = l$ es la característica del campo base; si p_{ii} es una raíz t-ésima primitiva de unidad, $t \neq 1$, entonces $h(i) = t$.*

El conjunto U se conoce como el conjunto de generadores PBW de H. Este teorema se sigue de [35, Teorema 2]. Revisaremos algunas nociones necesarias.

Sea $a_1, \dots, a_n$ el conjunto de elementos primitivos torcidos generadores de H, y sean x_i las variables cuánticas asociadas. Consideremos el ordenamiento lexicográfico de todas las palabras, $x_1 > x_2 > \dots > x_n$. El inicio de una palabra se considera mayor que la palabra misma, por ejemplo $x_1 > x_1 x_2^2 > x_1 x_2^2 x_1$. Una palabra no vacía se llama *estándar* si $vw > wv$ para cada descomposición $u = vw$ con v, w no vacías. Las siguientes son propiedades conocidas (véase [9], [12], [48], [63], [64]).

1. Una palabra u es estándar si y sólo si es mayor que cada uno de sus finales.
2. Toda palabra estándar comienza con la letra maximal que posee.
3. Cada palabra c tiene una representación única $c = u_1^{n_1} u_2^{n_2} \dots u_k^{n_k}$, donde $u_1 < u_2 < \dots < u_k$ son palabras estándar (teorema de Lyndon).
4. Si u, v son palabras estándar distintas y u^n contiene a v^k como subpalabra, $u^n = cv^k d$, entonces u contiene a v^k como subpalabra, $u = bv^k e$.

Una palabra *no asociativa* es una palabra en la que los corchetes [,] están arreglados de modo que muestran cómo aplica la multiplicación. Si $[u]$ denota una palabra no asociativa, entonces se denota por u a la palabra asociativa obtenida de $[u]$ al remover los corchetes. Por supuesto, en general, $[u]$ no está definida por u de forma única.

El conjunto de palabras *no asociativas estándar* se define como el conjunto más pequeño SL que contiene todas las variables x_i y satisface las siguientes propiedades:

1. Si $[u] = [[v]\,[w]] \in SL$ entonces $[v]$, $[w] \in SL$, y $v > w$ son estándar.
2. Si $[u] = [[[v_1]\,[v_2]]\,[w]] \in SL$, entonces $v_2 \leq w$.

Las siguientes afirmaciones son válidas también:

1. Toda palabra estándar tiene una alineación de corchetes única tal que la palabra asociativa en cuestión es estándar ([63, Teorema de Shirshov]).
2. Los factores v, w de la descomposición no asociativa $[u] = [[v]\,[w]]$ son palabras estándar tales que $u = vw$ y v tiene la longitud mínima ([64]).

3.14 Definición. Una *súper letra* es un polinomio que es igual a una palabra estándar no asociativa donde los corchetes son como (3.3). Una *súper palabra* es una palabra con súper letras.

Por el punto 2 recién expuesto, la palabra estándar u define la única súper letra, que en lo sucesivo denotaremos por $[u]$. Por ejemplo, las palabras $x_1x_2^2$, $x_2^3x_3$, $x_1x_2x_3x_2$, $x_2x_3x_2x_3x_4$, $x_1x_2x_3^2x_2$ son estándar y están definidas por las siguientes súper letras:

$$\left[x_1x_2^2\right] = [[x_1x_2]\,x_2]\,,\ \left[x_2^3x_3\right] = [x_2\,[x_2\,[x_2x_3]]]\,,\ [x_1x_2x_3x_2] = [[x_1\,[x_2x_3]]\,x_2]\,,$$

$$[x_2x_3x_2x_3x_4] = [[x_2x_3]\,[x_2\,[x_3x_4]]]\,,\ \left[x_1x_2x_3^2x_2\right] = [[x_1\,[[x_2x_3]\,x_3]]\,x_2]\,.$$

En el Teorema 3.7 teníamos que $W = \alpha\,[x_1x_2^n]$. Si las variables están ordenadas en forma opuesta, $x_2 > x_1$, entonces $x_1x_2^n$ no es una palabra estándar, mientras que $x_2^nx_1$ lo es, y se observa que $[\ldots[[x_1x_2]\,x_2]\ldots x_2] = (-p_{12})^n\,p_{22}^{\frac{n(n-1)}{2}}\,[x_2^nx_1]$ dado que una de las condiciones de existencia es válida (véase el Corolario 3.22). Por lo tanto, las relaciones cuantificadoras (3.10) pueden igualarse con cero para algunas súper letras:

$$\left[x_jx_i^{n_{ij}}\right] = 0,\ \left[x_j^{n_{ji}}x_i\right] = 0,\ j < i. \tag{3.15}$$

Sea D un grupo aditivo abeliano linealmente ordenado. Supongamos que algunos D-grados positivos $d_1, \ldots, d_n \in D$ están asociados a $x_1, \ldots, x_n$. Definiremos al grado de una palabra igual con $m_1d_1 + \ldots + m_nd_n$ donde $(m_1, \ldots, m_n)$ es la constitución de la palabra. El orden y el grado de las súper letras están definidas del siguiente modo: $[u] > [v] \Longleftrightarrow u > v; D\,([u]) = D\,(u)$.

3.15 Definición. Una súper letra $[u]$ se llama *dura* en H si su valor en H no es una combinación lineal de valores de súper palabras del mismo grado en menos de $[u]$ súper letras y G-súper palabras de menor grado.

3.16 Definición. Decimos que la *altura* de una súper letra $[u]$ de grado d es igual con $h = h\,([u])$ si h es el menor número tal que: primero p_{uu} es una raíz primitiva t-ésima de unidad y $h = t$ o $h = tl^r$, donde $l = \mathrm{char}\,(\mathbf{k})$; y entonces el valor en H de $[u]^h$ es una combinación de súper palabras de grado hd en menos que $[u]$ súper letras y G- súper palabras de menor grado. Si no existe tal número, entonces la altura es igual a infinito.

Si el álgebra H es D-homogénea, entonces pueden omitirse las partes subrayadas de las definiciones previas.

3.17 Teorema (Teorema 2,[35])**.** *El conjunto de todos los valores en H de todas las G-súper palabras W en las $[u_i]$ súper letras duras,*

$$W = g\,[u_1]^{n_1}\,[u_2]^{n_2}\ldots[u_m]^{n_m}\,, \tag{3.16}$$

donde $g \in G$, $u_1 < u_2 < \ldots < u_m$, $n_i < h\,([u_i])$ es una base de H.

Para encontrar el conjunto U de generadores PBW es necesario incluir en U los valores de todas las súper letras duras. Luego, para cada súper letra dura $[u]$ de una altura finita $h\,([u]) = tl^k$, añadir los valores de $[u]^t, [u]^{tl}, \ldots, [u]^{tl(k-1)}$, y después añadir el

valor de $[u]^t$ para cada súper letra dura de alturas infinitas tales que p_{uu} es una raíz t-ésima primitiva de unidad.

Naturalmente, el conjunto de generadores PBW juega el mismo rol que la base del álgebra de Lie en el teorema PBW. Sin embargo, el $\mathbf{k}[G]$-bimódulo generado por los generadores PBW no está definido de manera única. Depende del ordenamiento de los generadores principales, el grado D, y bajo la acción de la antípoda se transforma a un bimódulo diferente de generadores PBW $\mathbf{k}[G]S(U)$.

Otra forma de construir los generadores PBW está conectada con la idea de cristalización de M. Kashiwara [31], [32]. M. Kashiwara consideró el mayor parámetro del álgebra envolvente de Drinfeld-Jimbo como la temperatura de algún medio físico. Por esta razón emerge el término de *bases cristalizadas*. Si reemplazamos p_{ij} con cero, entonces $[u, v]$ se convierte en el monomio u, v, mientras que u se convierte en el monomio u.

3.18 Lema. *Bajo la cristalización monomial referida, el conjunto de generadores PBW construido en el Teorema 3.17 se convierte en otro conjunto de generadores PBW.*

Demostración. La prueba puede consultarse a detalle en [35, Corolario 1]. □

3.19 Lema. *Una súper letra $[u]$ es dura en H si y sólo si el valor de u no es una combinación lineal de valores de palabras menores del mismo grado y G-palabras de menor grado.*

Demostración. La demostración se encuentra en [35, Corolario 2]. □

3.20 Lema. *Sea B el conjunto de súper letras que contienen $x_1, \ldots, x_n$. Si cada par $[u]$, $[v] \in B$, $u > v$ satisface una de las siguientes condiciones:*

i) $[[u], [v]]$ *no es una palabra estándar no asociativa;*

ii) *la súper letra* $[[u][v]]$ *es no dura en H;*

iii) $[[u][v]] \in B$,

entonces el conjunto B incluye todas las letras súper duras en H.

Demostración. Sea $[w]$ una letra súper dura de grado minimal tal que $[w] \notin B$. Entonces $[w] = [[u]\,[v]]$, $u > v$ donde $[u]$, $[v]$ son súper letras duras. De hecho, si $[u]$ no es dura, entonces por el Lema 3.19 tenemos $u = \sum \alpha_i u_i + S$, donde $u_i < u$ y $D(u_i) = D(u)$, $D(S) < D(u)$. Tenemos $uv = \sum \alpha_i u_i v + Sv$, donde $u_i v < uv$. Por lo tanto, por el Lema 3.19, la súper letra $[w] = [uv]$ no puede ser dura en H, lo cual resulta una contradicción. De manera similar, si $[v]$ no es dura, entonces $v = \sum \alpha_i v_i + S$, $v_i < v$, $D(v_i) = D(v)$, $D(S) = D(v)$. Entonces, $uv = \sum \alpha_i u v_i + uS$, $uv_i < uv$, y de nuevo $[w]$ no puede ser dura.

Así, de acuerdo con la elección de $[w]$, obtenemos $[u]$, $[v] \in B$. Dado que este par satisface las condiciones *i)* y *ii)*, la condición *iii)*; $[uv] \in B$ se satisface. □

3.21 Lema. *Si* $\mathbf{T} \in H$ *es un elemento primitivo torcido, entonces*

$$\mathbf{T} = \alpha\,[u]^h + \sum \alpha_i W_i + \sum \beta_j g_j W_j', \quad \alpha \neq 0, \tag{3.17}$$

donde $[u]$ *es una súper letra dura,* W_i *son súper palabras base en súper letras menores que* $[u]$*,* $D(W_i) = hD([u])$*,* $D\left(W_j'+\right) < hD([u])$*. Aquí si* p_{uu} *no es una raíz de unidad, entonces* $h = 1$*; si* p_{uu} *es una raíz primitiva* t*-ésima de unidad, entonces* $h = 1$*, o* $h = t$*, o* $h = tl^k$*, donde* l *es la característica.*

Demostración. Consideremos una expansión de $\mathbf{T}$ en términos de la base (3.16)

$$\mathbf{T} = \alpha g U + \sum_{i=1}^{k} \gamma_i g_i W_i + W', \quad \alpha \neq 0, \tag{3.18}$$

donde gU, $g_i W_i$ son elementos base distintos de grado maximal, y U es una de las mayores palabras entre U, W_i con respecto al orden lexicográfico de palabras en las súper letras. En la expansión base de tensores, el elemento $\Delta(\mathbf{T}) - \mathbf{T} \otimes 1 - g_t \otimes \mathbf{T}$ tiene sólo un tensor de la forma $gU \otimes \ldots$ y este tensor es igual con $gU \otimes \alpha(g-1)$. Por lo tanto, $g = 1$ y es posible aplicar [35, Lema 13]. □

3.22 Corolario. *Si una de las condiciones de existencia en el Teorema 3.7 se satisface, entonces*

$$[\ldots[[x_1 x_2]\,x_2]\ldots x_2] = (-p_{12})^n\, p_{22}^{\frac{n(n-1)}{2}}\,[x_2\,[x_2 \ldots [x_2 x_1]\ldots]]\,.$$

Demostración. Introduzcamos el orden opuesto, $x_2 > x_1$. Puesto que $[\ldots[[x_1 x_2]\,x_2]\ldots x_2]$ es una operación cuántica de Lie, admite una representación como la expuesta en (3.17), donde todos los sumandos tienen la misma constitución, $(1, n)$. Esto implica que $h = 1$,

$u = x_2^n x_1$. Todas las palabras estándar de la constitución menores o iguales con $(1, n)$ son x_2, $x_2^k x_1$, $k \leq n$. Por definición del orden lexicográfico, $x_2 > x_2^n x_1$. Por lo tanto, x_2 no ocurre en (3.17) como súper letra. Dado que todo sumando es de grado 1 en x_1, la igualdad (3.17) se reduce a $\mathbf{T} = \alpha\,[x_2^n x_1]$. Para encontrar α, se puede comparar los coeficientes en $x_2^n x_1$. □

3.4. Relaciones de Groebner-Shirshov

Sean $x_1, \ldots, x_n$ variables con grados positivos $d_1, \ldots, d_n \in D$. Recordemos que el *ordenamiento de Hall* de palabras en $x_1, \ldots, x_n$ es un orden en el cual las palabras son comparadas primero por el grado y luego palabras del mismo grado se comparan por medio del orden lexicográfico. Consideremos un conjunto de relaciones

$$w_i = f_i, \quad i \in I, \tag{3.19}$$

donde w_i es una palabra y f_i es una combinación lineal de Hall de palabras menores. El sistema (3.19) se dice *cerrado bajo composiciones* o un *sistema de relaciones de Groebner-Shirshov* si, en primer lugar, ninguna de las w_i contiene a w_j, $i \neq j \in I$ como subpalabra, y entonces para cada par de palabras w_k, w_j tal que algunas terminales no vacías de w_k coinciden con el comienzo de w_j, esto es, $w_k = w'_k v$, $w_j = v w'_j$, la diferencia (*una composición*) $f_k w'_j - w'_k f_j$ puede reducirse a cero en el *álgebra libre* a través de la secuencia de sustituciones de un sólo lado $w_i \to f_i$, $i \in I$.

3.23 Lema (Lema del Diamante [5],[7],[64])**.** *Si el sistema* (3.19) *es cerrado bajo composición, entonces las palabras que no poseen a ninguna w_i como subpalabras forman una base del álgebra H definida en* (3.19)*.*

Si ninguna de las palabras w_i tiene subpalabras w_j, $j \neq i$, entonces la afirmación a la inversa también es válida. De hecho, cualquier composición por medio de sustituciones $w_i \to f_i$ puede reducirse a una combinación lineal de palabras que no tengan subpalabras w_i. Puesto que $f_i w'_i - w'_i f_j = (f_i - w_i)\, w'_j - w'_i\, (f_j - w_j)$, esta combinación lineal es igual con cero en H. Por lo tanto, todos los coeficientes deben ser cero.

Dado que el Lema 3.18 brinda la base que consiste de palabras, lo anterior da una manera de construir el sistema de relaciones Groebner-Shirshov para cualquier álgebra cuántica envolvente.

Sea H una álgebra de Hopf caracter generada por semiinvariantes primitivos torcidos $a_1, \ldots, a_n$ (o por álgebras de Hopf trenzadas biclasificadas generadas por elementos

primitivos homogéneos clasificados $a_1, \ldots, a_n$) y sean $x_1, \ldots, x_n$ las variables cuánticas asociadas. Una súper letra no dura en H $[w]$ se llama *minimal* si, primero, w no tiene subpalabras estándar propias que definan súper letras no duras y, luego, si w no tiene subpalabras u^h, donde $[u]$ es una súper letra dura de altura h.

Por el Lema 3.19, para toda súper letra minimal no dura $[w]$ en H es posible escribir la relación en H como

$$w = \sum \alpha_i w_i + \sum \beta_j g_j w_j, \tag{3.20}$$

donde w_j, $w_i < w$ en el sentido de Hall, $D(w_i) = D(w)$, $D(w_j) < D(w)$. De igual forma, si $[u]$ es una súper letra dura en H de una altura finita h, entonces

$$u^h = \sum \alpha_i u_i + \sum \beta_j g_j u_j, \tag{3.21}$$

donde u_j, $u_i < u^h$ en el sentido de Hall, $D(u_i) = hD(u)$, $D(u_j) < hD(u)$. Las relaciones (3.13) y la operación de grupo brindan las relaciones

$$x_i g = \chi^{x_i}(g)\, g x_i, \quad g_1 g_2 = g_3. \tag{3.22}$$

3.24 Teorema. *El conjunto de relaciones* (3.20), (3.21), *y* (3.22) *forma un sistema de Groebner-Shirshov que define a H. La base determinada por dicho sistema en el Lema del Diamante coincide con la base PBW obtenida por medio de una cristalización monomial.*

Demostración. La propiedad *iv*) implica que ninguno de los lados izquierdos de (3.20), (3.21) y (3.22) contiene a otra como subpalabra. Por el Lema 3.18 es suficiente con mostrar que el conjunto de todas las palabras c determinadas en el Lema del Diamante coincide con la base del Lema (A.18). Por *iii*) tenemos que $c = u_1^{n_1} u_2^{n_2} \ldots u_k^{n_k}$, donde $u_1 < \ldots < u_k$ es una secuencia de palabras estándar. Toda palabra u_i define una súper letra dura $[u_i]$ ya que en el caso opuesto u_i, y por lo tanto c, contiene una subpalabra w que define una súper letra minimal no dura $[w]$. Del mismo modo, n_i no excede la altura de $[u_i]$. □

3.25 Lema. *En términos del Lema 3.20, el conjunto de todas las súper letras $[[u]\,[v]]$ que satisfacen la condición ii) contiene todas las súper letras minimales no duras, pero generadores no duros x_i.*

Demostración. Si $[w]$ es una súper letra minimal no dura, entonces $[w] = [[u]\,[v]]$, donde $[u]$, $[v]$ son súper letras duras. Por el Lema 3.20 tenemos que $[u]$, $[v] \in B$, mientras que $[[u]\,,[v]]$ no satisface ni *i*) ni *iii*). □

3.5. Cuantificación con constantes

En algunas instancias la investigación de la cuantificación con constantes puede reducirse a una cuantificación por medio del Lema del Diamante.

Sea $H_1 = G\langle x_1, \dots, x_k || F_1\rangle$ el álgebra de Hopf caracter definida por las variables cuánticas $x_1, \dots, x_k$ y la clasificación por relaciones homogéneas $\{f = 0 : f \in F_1\}$; mientras que $H_2 = G\langle x_{k+1}, \dots, x_n\rangle$, la definida por las variables cuánticas $x_{k+1}, \dots, x_n$ y la clasificación por relaciones homogéneas $\{h = 0 : h \in F_2\}$. Consideremos el álgebra $H = G\langle x_1, \dots, x_n || F_1, F_2, F_3\rangle$, donde F_3 es el siguiente sistema de relaciones con constantes:

$$[x_i, x_j] = \alpha_{ij}(1 - g_i g_j), \quad 1 \le i \le k < j \le n. \tag{3.23}$$

Si las condiciones anteriores se satisfacen, entonces la estructura de álgebra de Hopf caracter en H está definida en forma única:

$$p_{ij}p_{ji} = 1, \quad 1 \le i \le k < j \le n; \quad \chi^{x_i}\chi^{x_j} \ne 1 \Rightarrow \alpha_{ij} = 0. \tag{3.24}$$

En este caso, la diferencia w_{ij} entre los lados izquierdo y derecho en (3.23) es un semiinvariante primitivo torcido del álgebra envolvente libre $G\langle x_1, \dots, x_n\rangle$. Consideremos los ideales de las relaciones $I_1 = \mathrm{id}(F_1)$ y $I_2 = \mathrm{id}(F_2)$ de H_1 y H_2, respectivamente. Éstos son, en el presente contexto, ideales de Hopf de $G\langle x_1, \dots, x_k\rangle$ y $G\langle x_{k+1}, \dots, x_n\rangle$, respectivamente. Por lo tanto $V = I_1 + I_2 + \sum \mathbf{k}[G] w_{ij}$ es un ideal antípoda estable de $G\langle X\rangle$. En consecuencia, el ideal generado por V es un ideal de Hopf. Cabe destacar que este ideal es generado en $G\langle X\rangle$ por w_{ij} y F_1, F_2.

3.26 Lema. *Toda súper letra dura H pertenece a H_1 o H_2, y es dura en el álgebra asociada.*

Demostración. Si una palabra estándar contiene al menos una de las letras x_i, $i \le k$, entonces debe comenzar con una de ellas (véase *ii*) en la sección §3.3). Si esta palabra contiene una letra x_j, $j > k$, entonces tiene una subpalabra de la forma $x_i x_j$, $i \le k < j$. Por lo tanto, por el Lema 3.19 y las relaciones (3.23), esta palabra define a una súper letra no dura. □

La afirmación a la inversa no es universalmente cierta. Para formular las condiciones suficientes y necesarias, definamos las derivadas parciales torcidas:

$$\partial_i(x_j) = \partial_j(x_i) = \alpha_{ij}(1 - g_i g_j), \quad 1 \le k < j; \tag{3.25}$$
$$\partial_i(v \cdot w) = \partial_i(v) \cdot w + p(x_i, v)\, v \cdot \partial_i(w), \quad i \le k, \quad v, w \in \mathbf{k}\langle x_{k+1}, \dots, x_n\rangle;$$
$$\partial_j(u \cdot v) = p(v, x_j)\, \partial_j(u) \cdot v + u \cdot \partial_j(v), \quad j > k, \quad u, v \in \mathbf{k}\langle x_1, \dots, x_k\rangle.$$

3.27 Lema. *Todas las súper letras duras en H_1 o H_2 son duras en H si y sólo si $\partial_i(h) = 0$ en H_2 para toda $i \leq k$, $h \in F_2$, y $\partial_j(f) = 0$ para toda $j > k$, $f \in F_1$. Si dichas condiciones se verifican, entonces*

$$H \cong H_2 \otimes_{k[G]} H_1 \tag{3.26}$$

como $\mathbf{k}[G]$-bimódulos, y el espacio generado por los elementos primitivos torcidos de H es igual a la suma de estos espacios para H_1 y H_2.

Demostración. Por (3.4) y (3.25) las siguientes igualdades son válidas en H:

$$0 = [x_i, h] = \partial_i(h); \quad 0 = [f, x_j] = \partial_j(f), \quad i \leq k < j. \tag{3.27}$$

Si todas las súper letras duras en H_1 o H_2 son duras en H, entonces H_1 y H_2 son subálgebras de H. De manera que (3.27) prueba la necesidad de las condiciones del lema.

A la inversa, consideremos una álgebra R definida por los generadores $g \in G$, $x_1, \ldots, x_n$ y las relaciones (3.22) y (3.23). Este sistema es cerrado bajo las composiciones. Por lo tanto, por el Lema del Diamante, el conjunto de palabras gvw forma una base de R donde $g \in G$; v es una palabra en x_j, $j > k$; y w es una palabra en x_i, $i \leq k$. En otras palabras R encuentra como bimódulo una descomposición de la forma

$$R = G\langle x_{k+1}, \ldots, x_n\rangle \otimes_{\mathbf{k}[G]} G\langle x_1, \ldots, x_k\rangle. \tag{3.28}$$

Consideremos que el ideal de R por ambos lados generado por F_2 coincide con el ideal derecho $I_2R = I_2 \otimes_{\mathbf{k}[G]} G\langle x_1, \ldots, x_k\rangle$. Es suficiente con probar que I_2R admite la multiplicación por la izquierda por x_i, $i \leq k$. Si v es una palabra en $x_{k+1}, \ldots, x_n$, $h \in F_2$, $r \in R$, entonces $x_ivhr = [x_i, vh]\, r + p(x_i, vh)\, vhx_ir$. El segundo término pertenece a I_2R, mientras que el primero puede ser reescrito con (3.4): $[x_i, v]\, h + p(x_i, v)\, v\, [x_i, h]$. Ambos de esos sumandos pertenecen a I_2R dado que $[x_i, v] = \partial_i(v) \in G\langle x_{k+1}, \ldots, x_n\rangle$ y $[x_i, h] = \partial_i(h) \in I_2$.

Además, consideremos el álgebra cociente $R_1 = R/I_2R$:

$$\begin{aligned} R_1 = {} & \left(G\langle x_{k+1}, \ldots, x_n\rangle \otimes_{\mathbf{k}[G]} G\langle x_1, \ldots, x_k\rangle\right) / \left(I_2 \otimes_{\mathbf{k}[G]} G\langle x_1, \ldots, x_k\rangle\right) \\ & H_2 \otimes_{\mathbf{k}[G]} G\langle x_1, \ldots, x_k\rangle, \end{aligned}$$

donde la igualdad significa el isomorfismo natural de $\mathbf{k}[G]$-bimódulos.

En el mismo orden de ideas, el ideal izquierdo $R_1I_1 = H_2 \otimes_{\mathbf{k}[G]} I_1$ de esta álgebra de cocientes con el ideal de ambos lados generado por F_1. Por lo tanto,

$$\begin{aligned} H &= R_1/R_1I_1 \\ &= H_2 \otimes_{\mathbf{k}[G]} G\langle x_1, \ldots, x_k\rangle / H_2 \otimes_{\mathbf{k}[G]} I_1 \\ &= H_2 \otimes_{\mathbf{k}[G]} H_1. \end{aligned}$$

□

Así, las G-palabras monótonas restringidas a ser duras en H_1 o H_2 como súper letras forman una base de H. Esto, en particular, prueba la primera afirmación.

Ahora, sea $T = \sum \alpha_t g_t V_t W_t$ la descomposición base de un elemento primitivo torcido, $g_t \in G$, $V_t \in H_2$, $W_t \in H_1$, $\alpha_t \neq 0$. Debe mostrarse que por cada t una de las súper palabras V_t o W_t está vacía. Supongamos que no es así. Entre los sumandos no vacíos V_t, W_t elegiremos al más grande en el sentido de Hall, por ejemplo $g_s V_s W_s$. Bajo la base de la descomposición de $\Delta(T) - T \otimes 1 - g(T) \otimes T$ aparece el término $\alpha_s g_s g(V_s) W_s \otimes g_s V_s$ y no puede ser cancelado por otro. De hecho, dado que el coproducto es homogéneo (véase [35, Lema 9]), y puesto que bajo la base de la descomposición las súper palabras decrecen (véase [35, Lema 7]), el producto $\alpha_s (g_s \otimes g_s) \Delta(V_s) \delta(W_s)$ tiene el único término con la forma recién expuesta. Por las mismas razones $\alpha_t (g_t \otimes g_t) \Delta(V_t) \delta(W_t)$ tiene un término como el expuesto si $V_t \geq V_s$ y $W_t \geq W_s$ con respecto al ordenamiento de Hall del conjunto de todas las súper palabras. Sin embargo, por la elección de s, tenemos que $D(V_s W_s) \geq D(V_t W_t)$. Así, $D(V_t) = D(V_s)$ y $D(W_t) = D(W_s)$. En particular, V_t no es un inicio propio de V_s. Por lo tanto, $V_t = V_s$ dado que de otra manera la desigualdad $V_t > V_s$ conduce a una contradicción, $V_t W_t > V_s W_s$. La desigualdad $W_t > W_s$ lleva a la misma contradicción. Por lo tanto, $V_t = V_s$ y $W_t = W_s$, en cuyo caso $g_t g(V_t) W_t \otimes g_t V_t = g_s g(V_s) W_s \otimes g_s V_s$. Así, $g_t = g_s$ y $t = s$.

Capítulo 4

El grupo cuántico $U_q^+(\mathfrak{so}_{2n+1})$

Todas las relaciones definitorias del grupo cuántico $U_q(\mathfrak{so}_{2n+1})$ son primitivas torcidas como polinomios no conmutativos con coeficientes de tipo grupo y, por esa razón, el ideal minimal J_1 contiene todas la relaciones de $U_q(\mathfrak{so}_{2n+1})$. Por lo tanto, en lugar del morfismo $H\langle X\rangle \to u_q(\mathfrak{so}_{2n+1})$ es posible considerar el morfismo $U_q(\mathfrak{so}_{2n+1}) \to u_q(\mathfrak{so}_{2n+1})$. Ello brinda la posibilidad de trabajar con elementos de $U_q(\mathfrak{so}_{2n+1})$ en lugar de emplear los polinomios no conmutativos generales.

En este capítulo se abordan conceptos asociados al grupo cuántico $U_q(\mathfrak{so}_{2n+1})$ con el fin de emplear la fórmula explícita del coproducto y algunos resultados estructurales en el capítulo siguiente en el que se hallará el rango combinatorio de la versión multiparamétrica del grupo cuántico de Lusztig pequeño $u_q(\mathfrak{so}_{2n+1})$.

4.1. Nociones preliminares

Sea A una álgebra sobre el campo $\mathbf{k}$ y B su subálgebra con una base fija $\{g_i | j \in J\}$. Recordemos que un subconjunto ordenado en forma lineal $V \subset A$ se dice que es un *conjunto de generadores PBW de A sobre B* si existe una función $h : V \to \mathbb{Z}^+ \cup \infty$, llamada la *función altura* tal que el conjunto de todos los productos

$$g_j v_1^{n_1} v_2^{n_2} \dots v_k^{n_k}, \tag{4.1}$$

donde $j \in J$, $v_1 < v_2 < \ldots < v_k \in V$, $n_i < h(v_i)$, $1 \leq i \leq k$ es una base de A. El valor $h(v)$ es el *peso* de $v \in V$.

Recordemos que una álgebra de Hopf H se llama *álgebra de Hopf caracter* si el grupo G de todos los elementos de tipo grupo es conmutativa y H es generada sobre $\mathbf{k}[G]$ por semi-invariantes primitivos torcidos a_i, $i \in I$:

$$\Delta(a_i) = a_i \otimes 1 + g_i \otimes a_i, \quad g^{-1} a_i g = \chi^i(g)\, a_i, \quad g, g_i \in G, \tag{4.2}$$

donde χ^i, $i \in I$ son caracteres del grupo G. Por medio del Lema de Dedekind se observa que toda álgebra de Hopf caracter está clasificada por el monoide G^* de caracteres generados por χ^i :

$$H = \sum_{\chi \in G^*} \oplus H^\chi, \quad H^\chi = \left\{ a \in H | g^{-1} a g = \chi(g)\, a,\ g \in G \right\}. \tag{4.3}$$

Asociemos a las a_i una variable cuántica x_i. Para cada palabra $u \in X = \{x_i | i \in I\}$ denotamos por g_u o $\mathrm{gr}(u)$ a un elemento de G que aparece en u al reemplazar cada x_i con g_i. De igual manera, denotamos con χ^u un caracter que aparece en u cuando se reemplaza cada x_i con χ^i. Definimos un conmutador bilineal torcido en combinaciones lineales homogéneas de palabras en a_i o en x_i, $i \in I$ con la fórmula

$$[u, v] = uv - \chi^u(g_v)\, vu, \tag{4.4}$$

donde emplearemos también la notación $\chi^u(g_v) = p_{uv} = p(u, v)$. Se tiene que $p(u, v)$ es un mapeo bimultiplicativo:

$$p(u, vt) = p(u, v)\, p(u, t), \quad p(ut, v) = p(u, v)\, p(t, v). \tag{4.5}$$

Como mencionamos en el capítulo anterior, los corchetes satisfacen la identidad de Jacobi:

$$[[u, v], w] = [u, [v, w]] + p_{wv}^{-1} [[u, w], v] + \left(p_{vw} - p_{wv}^{-1}\right) [u, w] \cdot v \tag{4.6}$$

o, de forma equivalente, en otra forma menos simétrica

$$[[u, v], w] = [u, [v, w]] + p_{vw} [u, w] \cdot v - p_{uv} v \cdot [u, w]. \tag{4.7}$$

La identidad de Jacobi (4.6) implica la identidad condicional

$$[[u, v], w] = [u, [v, w]], \text{ si } [u, w] = 0. \tag{4.8}$$

Por medio de inducción sobre la longitud de esta identidad condicional se verifica la siguiente generalización, ([43, Lema 2.2]).

4.1 Lema. *Si $y_1, y_2, \ldots, y_m$ son combinaciones lineales homogéneas de palabras tales que $[y_i, y_j] = 0$, $i \leq i < j - 1 < m$, entonces el polinomio $[y_1 y_2 \ldots y_m]$ es independiente de la alineación de los corchetes:*

$$[y_1 y_2 \ldots y_m] = [[y_1 y_2 \ldots y_s], [y_{s+1} y_{s+2} \ldots y_m]], \quad 1 \leq s < m. \tag{4.9}$$

Los corchetes están relacionados con el producto mediante las identidades

$$[u \cdot v, w] = p_{vw} [u, w] \cdot v + u \cdot [v, w], \tag{4.10}$$
$$[u, v \cdot w] = [u, v] \cdot w + p_{uv} v \cdot [u, w]. \tag{4.11}$$

En particular, si $[u, w] = 0$, tenemos que

$$[u \cdot v, w] = u \cdot [v, w]. \tag{4.12}$$

La identidad antisimétrica se transforma en las siguientes dos igualdades

$$[u, v] = -p_{vu} [v, u] + (1 - p_{uv} p_{vu}) u \cdot v, \tag{4.13}$$
$$[u, v] = -p_{vu}^{-1} [v, u] + \left(p_{vu}^{-1} - p_{uv}\right) v \cdot u. \tag{4.14}$$

En particular, si $p_{uv} p_{vu} = 1$ (la antisimetría coloreada) $[u, v] = -p_{uv} [v, u]$ se cumple.

El grupo G actúa en el álgebra libre $\mathbf{k} \langle X \rangle$ por medio de $g^{-1} u g = \chi^u (g) u$, donde u es un monomio arbitrario en X. El álgebra torcida $G \langle X \rangle$ tiene la estructura natural de una álgebra de Hopf

$$\Delta (x_i) = x_i \otimes 1 + g_i \otimes x_i, \quad i \in I, \quad \Delta (g) = g \otimes g, \ g \in G.$$

Fijaremos un homomorfismo de una álgebra de Hopf

$$\epsilon : G \langle X \rangle \to H, \quad \epsilon (x_i) = a_i, \quad \epsilon (g) = g, \quad i \in I, \quad g \in G. \tag{4.15}$$

La *constitución* de una palabra u en $B \cup X$ es una familia de enteros no negativos $\{m_x, x \in X\}$ tales que u tiene m_x ocurrencias de x. Ciertamente, casi todas las m_x en

la constitución son cero. Fijemos un orden arbitrario completo, $<$, en el conjunto X. Normalmente, si $X = \{x_1, \ldots, x_n\}$, estableceremos que $x_1 > x_2 > \ldots > x_n$.

Sea Γ^+ el monoide libre aditivo libre (conmutativo) generado por X. El monoide Γ^+ es un monoide completamente ordenado con respecto al siguiente orden:

$$m_1 x_{i_1} + m_2 x_{i_2} + \ldots + m_k x_{i_k} > m'_1 x_{i_1} + m'_2 x_{i_2} + \ldots + m'_k x_{i_k} \tag{4.16}$$

si el primer número a la izquierda en $(m_1 - m'_1, m_2 - m'_2, \ldots + m_k - m'_k)$ es positivo, donde $x_{i_1} > x_{i_2} > \ldots > x_{i_k}$ en X. Asociemos un grado formal $D(u) = \sum_{x \in X} m_x x \in \Gamma^+$ a una palabra u en $G \cup X$, donde $\{m_x | x \in X\}$ es la constitución de u. Respectivamente, si $f = \sum \alpha_i u_i \in G\langle X \rangle$, $0 \neq \alpha_i \in \mathbf{k}$, entonces

$$D(f) = \max_i \{D(u_i)\}. \tag{4.17}$$

Conviene tener presente el siguiente algoritmo, mismo que será de utilidad más adelante: los factores v, w de la descomposición no asociativa $[u] = [[v], [w]]$ son las palabras estándar tales que $u = vw$ y v con longitud mínima (véase [64] y [49]).

Retomando los conceptos de palabra estándar no asociativa, súper letra, súper letra dura y su respectiva altura, expuestos en el capítulo previo, recordemos un resultado fundamental para estudiar la base PBW para subálgebras homogéneas de coideal derecho.

4.2 Teorema (Teorema 2, [35])**.** *Los valores de todas las súper letras en H con la función altura forman un conjunto de generadores PBW para H sobre $\mathbf{k}[G]$.*

El conjunto T de generadores PBW para subálgebras homogéneas de coideal derecho $\mathbf{U}$, $\mathbf{k}[G] \subset \mathbf{U} \subset H$, puede obtenerse de la base PBW dada en el Teorema 4.2 en la siguiente forma (véase [39, Teorema1.1]).

Supongamos que para una súper letra dura $[u]$ existe un elemento homogéneo $c \in \mathbf{U}$ con el término líder $[u]^s$ en la descomposición PBW dada en el Teorema 4.2:

$$c = [u]^s + \sum_i \alpha_i W_i \in \mathbf{W}, \tag{4.18}$$

donde W_i es la base de súper palabras que comienzan con menos de $[u]$ súper letras. Fijemos uno de los elementos con la s minimal, y denotémoslo con c_u. Así, para cada súper letra dura $[u]$ en H tenemos a lo más un elemento c_u. Definamos la función altura por medio del siguiente lema.

4.3 Lema (Lema 4.3,[39]). *En la representación* (4.18) *del elemento elegido* c_u, $s = 1$ *o* $p(u,u)$ *es una raíz primitiva* t*-ésima de* 1 *y* $s = t$ *o (en el caso de que la característica sea positiva)* $s = t\,(\mathrm{char}\ \mathbf{k})^r$.

Si la altura de $[u]$ en H es infinita, entonces la altura de c_u en $\mathbf{U}$ se define también como infinita. Si la altura de $[u]$ en H es igual con t, entonces, gracias al lema anterior, $s = 1$ (en la descomposición PBW (4.18) el exponente s debe ser menor que la altura de $[u]$). En este caso la altura de c_u en $\mathbf{U}$ se supone también como t. Si la característica l es positiva, y la altura de $[u]$ en H es igual con tl^r, entonces definimos la altura de c_u en $\mathbf{U}$ igual a tl^r/s.

4.4 Proposición (Proposición 4.4,[39]). *El conjunto de todas las* c_u *elegidas conforme a la función altura recién definida forma un conjunto de generadores PBW para* $\mathbf{U}$ *sobre* $\mathbf{k}[G]$.

Recordemos que la base PBW no está definida en forma única en el proceso descrito. Sin embargo, el conjunto de términos líderes de los generadores PBW sí lo están.

4.5 Definición. El grado $sD(c_u) \in \gamma^+$ de un generador PBW c_u se dice que es una $\mathbf{U}$*-raíz*. Una $\mathbf{U}$-raíz $\gamma \in \Gamma^+$ se llama *simple* si no resulta la suma de dos o más $\mathbf{U}$-raíces.

El conjunto de $\mathbf{U}$-raíces, y el conjunto de $\mathbf{U}$-raíces simples son invariantes para cualquier subálgebra de coideal derecho $\mathbf{U}$.

Si el kernel de ϵ definido en (4.15) está contenido en el ideal $G\langle X\rangle^2$ generado por $x_i x_j$, $i,j \in I$, entonces existe una proyección del álgebra de Hopf $\pi : H \to \mathbf{k}[G]$, $a_i \to 0$, $g_i \to g_i$. Por el Teorema de Radford [58], tenemos una descomposición en un biproducto, $H = A\#\mathbf{k}[G]$, donde A es una subálgebra generada por a_i, $i \in I$, véase [1, §1.5,§1.7].

4.6 Definición. En adelante denotaremos con $\mathbf{\Lambda}$ al mayor ideal de Hopf en $G\langle X\rangle^{(2)}$, donde $G\langle X\rangle^{(2)}$ es el ideal de $g\langle X\rangle$ generado por $x_i x_j$, $i,j \in I$. El ideal $\mathbf{\Lambda}$ es homogéneo en cada $x_i \in X$, (véase [42, Lema 2.2]).

Si $\ker \epsilon = \mathbf{\Lambda}$ o, de manera equivalente, si A es una álgebra cuántica simétrica (una álgebra de Nichols [1, §1.3, Sección 2]), entonces A encuentra una representación barajada como se describe a continuación.

El álgebra A tiene la estructura de una *álgebra de Hopf trenzada*, [72], con un trenzado $\tau(u \otimes v) = p(v,u)^{-1} v \otimes u$. El coproducto trenzado Δ^b en A está conectado con el coproducto en H de la siguiente forma

$$\Delta^b(u) = \sum_{(u)} u^{(1)} \mathrm{gr}\left(u^{(2)}\right)^{-1} \underline{\otimes} u^{(2)}. \tag{4.19}$$

El espacio tensorial $T(V)$, $V = \sum x_i \mathbf{k}$ también tiene la estructura de una álgebra de Hopf trenzada. Esta es el *álgebra cuántica barajada* $Sh_\tau(V)$ con el coproducto

$$\Delta^b(u) = \sum_{i=0}^{m} (z_1 \dots z_i) \underline{\otimes} (z_{i+1} \dots z_m), \tag{4.20}$$

donde $z_i \in X$, y $u = (z_1 z_2 \dots z_{m-1} z_m)$ es el tensor $z_1 \otimes z_2 \otimes \dots \otimes z_{m-1} \otimes z_m$ considerado como un elemento de $Sh_\tau(V)$. El producto barajado satisface

$$(w)(x_i) = \sum_{uv=w} p(x_i, v)^{-1} (u x_i v), \quad (x_i)(w) = \sum_{uv=w} p(u, x_i)^{-1} (u x_i v). \tag{4.21}$$

El mapeo $a_i \to (x_i)$ define una incrustación del álgebra de Hopf trenzada A en el álgebra de Hopf trenzada $Sh_\tau(V)$. Esta incrustación es muy útil para calcular el coproducto gracias a las fórmulas (4.19), (4.20).

Otra noción importante es la del cálculo diferencial en nuestro contexto. El álgebra libre $\mathbf{k}\langle X\rangle$ tiene asociado un cálculo diferencial

$$\partial_j(x_i) = \delta_i^j, \quad \partial_i(uv) = \partial_i(u) \cdot v + \chi^u(g_i)\, u \cdot \partial_i(v). \tag{4.22}$$

Las derivadas parciales conectan al cálculo con el coproducto en $\mathbf{k}\langle X\rangle$ de la siguiente forma

$$\Delta(u) \equiv u \otimes 1 + \sum_i g_i \partial_i(u) \otimes x_i \quad \left(\mathrm{mod}\ G\langle X\rangle \otimes \mathbf{k}\langle X\rangle^{(2)}\right), \tag{4.23}$$

donde $\mathbf{k}\langle X\rangle^{(2)}$ es el ideal generado por $x_i x_j$, $1 \le i, j \le n$.

4.7 Lema. *Sea $u \in \mathbf{k}\langle X\rangle$ un elemento homogéneo en cada x_i. Si p_{uu} es una raíz primitiva t-ésima de unidad, entonces*

$$\partial_i\left(u^t\right) = p(u, x_i)^{t-1} \underbrace{[u, [u, \dots [u,}_{t-1} \partial_i(u)] \dots]]. \tag{4.24}$$

Demostración. Primero, haremos notar que la secuencia $p_{uu}, p_{uu}^2, \dots, p_{uu}^{t-1}$ contiene todas las raíces t-ésimas de 1 excepto el propio 1. Todos los miembros en esta secuencia

son distintos. Entonces, podemos escribir una igualdad polinomial

$$\left(1-x^t\right)=(1-x)\prod_{s=1}^{t-1}\left(1-p_{uu}^s x\right). \tag{4.25}$$

Calculemos el lado derecho de (4.24). Denotemos con L_u, R_u los operadores de multiplicación por u por la izquierda y por la derecha, respectivamente. El lado derecho de (4.24) tiene la siguiente representación como operador

$$p\left(u,x_i\right)^{t-1}\left(\partial_i\left(u\right)\cdot\prod_{s=1}^{t-1}\left(L_u-Qp_{uu}^{s-1}Ru\right)\right),$$

donde $Q=p\left(u,\partial_i\left(u\right)\right)=p_{uu}p\left(u,x_i\right)^{-1}$. Consideremos el polinomio

$$f\left(\lambda\right)=\prod_{s=1}^{t-1}\left(1-Qp_{uu}^{s-1}\lambda\right)\overset{\text{def}}{=}\sum_{k=0}^{t-1}\alpha_k\lambda^k.$$

Dado que los operadores R_u y L_u conmutan, podemos desarrollar la multiplicación en el operador producto considerando R_u y L_u como variables conmutativas:

$$\prod_{s=1}^{t-1}\left(L_u-Qp_{uu}^{s-1}Ru\right)=L_u^{t-1}f\left(\frac{R_u}{L_u}\right)=\sum_{k=0}^{t-1}\alpha_k L_u^{t-1-k}R_u^k.$$

Así, el lado derecho de (4.24) es igual con

$$p\left(u,x_i\right)^{t-1}\sum_{k=0}^{t-1}\alpha_k u^{t-1-k}\partial_i\left(u\right)u^k.$$

Por otra parte, puesto que $Q=p_{uu}p\left(u,x_i\right)^{-1}$, el polinomio f tiene una representación

$$f\left(\lambda\right)=\prod_{s=1}t-1\left(1-p_{uu}^s\epsilon\right),$$

donde $\epsilon=\lambda p\left(u,x_i\right)^{-1}$. Tomando en cuenta (4.25) se sigue que

$$\begin{aligned}f\left(\lambda\right)&=\frac{1-\epsilon^t}{1-\epsilon}\\&=\frac{1-\lambda^t p\left(u,x_i\right)^{-t}}{1-\lambda p\left(u,x_i\right)^{-1}}\\&=1+\lambda p\left(u,x_i\right)^{-1}+\lambda^2 p\left(u,x_i\right)^{-2}+\ldots+\lambda^{t-1}p\left(u,x_i\right)^{1-t};\end{aligned}$$

esto es, $\alpha = p(u, x_i)^{-k}$, mientras que el lado derecho de (4.24) toma la forma

$$\sum_{k=0}^{t-1} p(u, x_i)^{t-1-k} u^{t-1-k} \partial_i(u) u^k. \tag{4.26}$$

Al mismo tiempo, la fórmula de Leibniz (4.22) muestra que $\partial_i(u^t)$ también es igual con (4.26). □

Terminaremos este apartado haciendo una breve revisión al criterio de Milinski-Schneider y exponiendo algunos conceptos relacionados con el álgebra cuántica de Borel.

El álgebra cuántica simétrica tiene una serie de caracterizaciones. Una de ellas la describe como el *álgebra óptima* para el cálculo definido en (4.22). En otras palabras, el álgebra A definida recién es una álgebra cuántica simétrica (o, de forma equivalente, con $\ker \epsilon = \mathbf{\Lambda}$) si y sólo si todas las constantes en A son escalares. Para trenzados del tipo de Cartan esta caracterización fue probada por A. Milinski y H. J. Schneider en [53], y luego fue generalizada para trenzados arbitrarios (incluso para los no necesariamente invertibles) por Kharchenko en [38, Teorema 4.11]. Por otro lado, si X es finita, entonces $\mathbf{\Lambda}$, así como cualquier ideal diferencial en $\mathbf{k}\langle X\rangle$, es generado como un ideal de izquierda por constantes de $\mathbf{k}\langle X\rangle^{(2)}$ (véase [38, Corolario 7.8]). Así, puede formularse el siguiente criterio que resulta útil para revisar relaciones.

4.8 Lema (Criterio de Milinski-Schneider)**.** *Supongamos que* $\ker \epsilon = \mathbf{\Lambda}$*. Si el polinomio* $f \in \mathbf{k}\langle X\rangle$ *es una constante en* A *(esto es,* $\partial_i(f) \in \mathbf{\Lambda}$*,* $i \in I$*), entonces existe* $\alpha \in \mathbf{k}$ *tal que* $f - \alpha = 0$ *en* A*.*

Este criterio puede probarse empleando (4.19), (4.20) y (4.23) por medio de la representación barajada, ya que (4.20) implica que todas las constantes en la coálgebra barajada son escalares.

Ahora bien, sea $C = \|a_{ij}\|$ simetrizable por medio de la matriz de Cartan generalizada $D = \operatorname{diag}(d_1, \ldots, d_n)$, $d_i a_{ij} = d_j a_{ji}$. Denotemos ahora con $\mathfrak{g}$ al álgebra de Kac-Moody definida por C (véase [30]). Supongamos que los parámetros p_{ij} están relacionados de la siguiente manera

$$p_{ii} = q^{d_i}, \quad p_{ij}p_{ji} = q^{d_i a_{ij}}, \quad 1 \leq i, j \leq n. \tag{4.27}$$

Denotemos con g_j una transformación lineal $g_j : x_i \to p_{ij}x_i$ del espacio lineal generado por un conjunto de variables $X = \{x_1, x_2, \ldots, x_n\}$. Por χ^i denotamos el caracter $\chi^i : g_j \to p_{ij}$ del grupo G generado por g_i, $1 \leq i \leq n$. Consideremos cada x_i como variable

cuántica con parámetros g_i, χ^i. Como anteriormente, denotemos con $G\langle X\rangle$ el álgebra de grupo torcida con reglas de conmutación $x_i g_j = p_{ij} g_j x_i$, $1 \leq i, j \leq n$. Esta álgebra tiene la estructura de una álgebra de Hopf caracter

$$\Delta(x_i) = x_i \otimes 1 + g_i \otimes x_i, \quad \Delta(g_i)\, g_i \otimes g_i. \tag{4.28}$$

En este caso, la cuantificación multiparamétrica $U_q^+(\mathfrak{g})$ de la subálgebra de Borel $\mathfrak{g}^+$ es una imagen homomórfica de $G\langle X\rangle$ definida por las relaciones de Serre con los corchetes torcidos en lugar de la operación de Lie:

$$[\ldots[[x_i, \underbrace{x_j], x_j], \ldots, x_j}_{1-a_{ji} \text{ veces}}] = 0, \quad 1 \leq i \neq j \leq n. \tag{4.29}$$

Por [34, Teorema 6.1], los lados izquierdos de dichas relaciones son elementos torcidos primitivos en $G\langle X\rangle$. Por lo tanto, el ideal generado por esos elementos es un ideal de Hopf, en tanto que $U_q^{+(\mathfrak{g})}$ tiene una estructura natural de álgebra de Hopf caracter.

4.9 Lema (Corolario 3.2, [43])**.** *Si q no es una raíz de 1 y C es de tipo finito, entonces toda subálgebra U de $U_q^+(\mathfrak{g})$ que contenga a G es homogénea con respecto a cada una de las variables x_i.*

4.10 Definición. Si el orden multiplicativo t de q es finito, entonces definimos $u_q^+(\mathfrak{g})$ como $G\langle X\rangle/\mathbf{\Lambda}$, donde $\mathbf{\Lambda}$ es el mayor ideal de Hopf en $G\langle X\rangle^{(2)}$ (véase Definición 4.6).

Puesto que un elemento torcido primitivo genera un ideal de Hopf, $\mathbf{\Lambda}$ contiene todos los elementos torcidos primitivos de $G\langle X\rangle^{(2)}$. De manera que las relaciones (4.29) son también válidas en $u_q^+(\mathfrak{g})$.

4.2. Relaciones del álgebra cuántica de Borel $U_q^+(\mathfrak{so}_{2n+1})$

En adelante mantendremos fijo un parámetro q tal que $q^4 \neq 1$, $q^3 \neq 1$. Si C es una matriz de Cartan de tipo B_n, las relaciones (4.27) adquieren la forma

$$p_{nn} = q,\ p_{ii} = q^2,\ p_{ii+1}p_{i+1i} = q^{-2},\ 1 \leq i < n; \tag{4.30}$$

$$p_{ij}p_{ji} = 1\ j > i+1. \tag{4.31}$$

Comenzando con parámetros p_{ij} que satisfacen dichas relaciones, definamos el grupo G y al álgebra de Hopf caracter $G\langle X\rangle$ como lo hicimos recién. En este caso el álgebra cuántica de Borel $U_q^+(\mathfrak{so}_{2n+1})$ es la imagen homomórfica de $G\langle X\rangle$ sujeta a las siguientes relaciones

$$[x_i,[x_i,x_{i+1}]]=0,\ 1\le i<n;\quad [x_i,x_j]=0,\ j>i+1; \tag{4.32}$$

$$[[x_i,x_{i+1}],x_{i+1}]=[[[x_{n-1},x_n],x_n],x_n]=0,\ 1\le i<n-1. \tag{4.33}$$

Las relaciones de Serre (4.29) se han modificado ligeramente de forma tal que el lado izquierdo de cada relación es una súper letra. Esto es posible gracias a la relación general en $\mathbf{k}\langle X\rangle$ (véase [37, Corolario 4.10]):

$$[\dots[[x_i,\ \underbrace{x_j],x_j]\dots x_j]}_{n}=\alpha\underbrace{[x_j,[x_j,\dots[x_j}_{n}\ ,x_i]\dots]],\quad 0\neq\alpha\in\mathbf{k}, \tag{4.34}$$

dado que $p_{ij}p_{ji}=p_{jj}^{1-n}$.

4.11 Definición. Se dice que los elementos u, v son *separados* si existe un subíndice j, $1\le j\le n$, tal que $u\in\mathbf{k}\langle x_i|i<j\rangle$, $v\in\mathbf{k}\langle x_i|i>j\rangle$ o viceversa: $u\in\mathbf{k}\langle x_i|i>j\rangle$, $v\in\mathbf{k}\langle x_i|i<j\rangle$.

4.12 Lema. *En el álgebra $U_q^+(\mathfrak{so}_{2n+1})$ cada dos elementos homogéneos separados u, v en cada $x_i\in X$ son conmutativos torcidos: $[u,v]=[v,u]=0$.*

Demostración. Las relaciones (4.31) y la antisimetría condicional (4.14) muestra que $[x_i,x_j]=[x_j,x_i]=0$, ya que $|i-j|>1$. Gracias a las relaciones (4.10) y (4.11) es posible aplicar inducción para obtener el resultado. □

Ciertamente, la subálgebra de $U_q^+(\mathfrak{so}_{2n+1})$ generada sobre $\mathbf{k}[g_1,\dots,g_{n-1}]$ por x_i, $1\le i<n$ es el álgebra de Hopf $U_{q^2}^+(\mathfrak{sl}_n)$ definida por la matriz de Cartan de tipo A_{n-1}. Reemplacemos sólo un parámetro $p_{nn}\leftarrow q^2$. Entonces, el álgebra cuántica de Borel $U_{q^2}^+(\mathfrak{sl}_{n+1})$ es la imagen homomórfica de $G'\langle X\rangle$ sujeta a las relaciones

$$[[x_i,x_{i+1}],x_{i+1}]=[x_i,[x_i,x_{i+1}]]=[x_i,x_j]=0\quad j>i+1. \tag{4.35}$$

Aquí, G' es el grupo generado por transformaciones $g_1,\dots,g_{n-1},g_n'$, donde $g_n'(x_i)=g_n(x_i)$ con sólo una excepción, siendo $g_n'(x_n)=q^2x_n$.

4.13 Lema. *Una relación lineal $f=0$, en x_i, $f\in\mathbf{k}\langle X\rangle$ es válida en $U_q^+(\mathfrak{so}_{2n+1})$ si y sólo si es válida en el álgebra $U_{q^2}^+(\mathfrak{sl}_{n+1})$.*

Demostración. El elemento f, como elemento de una álgebra libre, pertenece al ideal generado por las relaciones definitorias que son independientes de x_n o lineales en x_n. Todas las relaciones son las mismas para $U_q^+(\mathfrak{so}_{2n+1})$ y para $U_{q^2}^+(\mathfrak{sl}_{n+1})$. □

4.14 Lema. *Si u es una palabra estándar, entonces $u = x_k x_{k+1} \dots x_m$, $k \leq m \leq n$ o $[u] = 0$ en $U_{q^2}^+(\mathfrak{sl}_{n+1})$. Aquí, $[u]$ es una palabra no asociativa con la alineación estándar de corchetes.*

Demostración. El resultado se sigue del Teorema A_n. □

Como corolario de los dos lemas anteriores, se tienen algunas relaciones en $U_q^+(\mathfrak{so}_{2n+1})$:

$$[[x_{k+1}x_k x_{k-1}], x_k] = 0 \quad [[x_{k-1}x_k x_{k+1}], x_k] = 0 \quad k < n. \tag{4.36}$$

De hecho, $x_{k-1}x_k x_{k+1}x_k$ es una palabra estándar y la alineación estándar de corchetes es precisamente $[[x_{k-1}, [x_k, x_{k+1}]], x_k]$. Por consiguiente, (4.8) junto con los lemas 4.13 y 4.14 implican la última relación.

La primera relación se reduce a la última al hacer el reemplazo $x_i \leftarrow x_{n-i+1}$, $1 \leq i \leq n$, $k \leftarrow n-k+1$. Resta destacar que las relaciones definitorias (4.35) son invariantes bajo este reemplazo (véase (4.34)) y hacen uso de los lemas 4.13 y 4.14.

4.15 Definición. En adelante denotaremos con x_i, $n < i \leq 2n$ al generador x_{2n-i+1}. $u(k,m)$, $1 \leq k \leq m \leq 2n$ es la palabra $x_k x_{k+1} \dots x_{m-1}x_m$, mientras que $u(m,k)$ es la palabra $x_m x_{m-1} \dots x_{k+1}x_k$. Si $1 \leq i \leq 2n$, entonces denotaremos con $\psi(i)$ al número $2n-i+1$, de manera que $x_i = x_{\psi(i)}$. Con frecuencia, deberemos emplear las siguientes propiedades de ψ: si $i < j$, entonces $\psi(i) > \psi(j)$; $\psi(\psi(i)) = i$; $\psi(i+1) = \psi(i) - 1$.

4.16 Definición. Si $k \leq i < m \leq 2n$, entonces denotamos

$$\sigma_k^m \stackrel{\text{def}}{=} p(u(k,m), u(k,m)), \tag{4.37}$$

$$\mu_k^{m,i} \stackrel{\text{def}}{=} p(u(k,i), u(i+1,m)) \cdot p(u(i+1,m), u(k,i)). \tag{4.38}$$

Es posible hallar a las μ y σ por medio de (4.30) y (4.31). Resulta que dichos coeficientes dependen solamente de q. De forma más precisa,

$$\sigma_k^m = \begin{cases} q, & \text{si } m = n \text{ o } k = n+1; \\ q^4, & \text{si } m = \psi(k); \\ q^2, & \text{en otro caso.} \end{cases} \tag{4.39}$$

En efecto, la bimultiplicatividad de $p(-,-)$ implica que $\sigma_k^m = \prod_{k\leq s,t\leq m} p_{st}$ es el producto de todos los coeficientes de la matriz $\|p_{st}\|$ de $(m-k+1)\times(m-k+1)$. Por (4.30) todos los coeficientes en la diagonal principal son iguales con q^2 con sólo dos excepciones posibles: $p_{nn} = q$ y $p_{n+1n+1} = q$. En particular, si $m < n$ o $k > n+1$, entonces para los coeficientes que no se encuentran en la diagonal tenemos que $p_{st}p_{ts} = 1$ a menos que $|s-t| = 1$, en tanto que $p_{ss+1}p_{s+1s} = q^{-2}$. Por lo tanto, $\sigma_k^m = q^{2(m-k+1)}\cdot q^{-2(k-m)} = q^2$. Si $m = n$ o $k = n+1$, entonces por la misma razón tenemos que $\sigma_k^m = q^{2(m-k)+1}\cdot q^{-2(k-m)} = q$. En el caso restante, $k \leq n < m$, partimos la matriz en cuatro matrices de la siguiente forma

$$\sigma_k^m = \sigma_k^n \cdot \sigma_{n+1}^m \cdot \prod_{k\leq s\leq n, n+1\leq t\leq m} p_{st} \cdot \prod_{n+1\leq s\leq m, k\leq t\leq n} p_{st}. \tag{4.40}$$

De acuerdo con la Definición (4.34), tenemos que $p_{st} = p_{\psi(s)t} = p_{s\psi(t)} = p_{\psi(s)\psi(t)}$. Por lo tanto, las afirmaciones tercera y cuarta en (4.30) respectivamente son iguales con

$$\prod_{k\leq s\leq n, \psi(m)\leq y\leq n} p_{st}; \qquad \prod_{\psi(m)\leq s\leq n, k\leq t\leq n} p_{st}.$$

En particular, si $\psi(m) = k$, entonces los cuatro factores en (4.40) coinciden con $\sigma_k^n = q$, por lo que $\sigma_k^m = q^4$. Si $\psi(m) \neq k$, digamos $\psi(m) > k$, entonces partimos la matriz rectangular $A = [k,n]\times[\psi(m),n]$ en la unión de la matriz cuadrada $B = [\psi(m),n]\times[\psi(m),n]$ y la matriz rectangular $C = [k,\psi(m)-1]\times[\psi(m),n]$. De manera similar, la matriz $A^* = [\psi(m),n]\times[k,n]$ es la unión de la misma matriz cuadrada y la matriz rectangular $c^* = [\psi(m),n]\times[k,\psi(m)-1]$.

Ciertamente, si $(s,t)\in C$, entonces $t-s>1$ a menos que $t = \psi(m)-1$, $s = \psi(m)$. En consecuencia, las relaciones (4.31) implican que

$$\prod_{(s,t)\in C} p_{st}p_{ts} = p_{\psi(m)-1\psi(m)}p_{\psi(m)\psi(m)-1} = q^{-2}.$$

al mismo tiempo, $\prod_{(s,t)\in B} p_{st} = \sigma_{\psi(m)}^n = q$. Finalmente, (4.40) toma la forma

$$\sigma_k^m = q\cdot q\left(\prod_{(s,t)\in B} p_{st}\right)^2 \cdot \prod_{(s,t)\in C} p_{st}p_{ts} = q^2,$$

lo cual prueba (4.39). Para encontrar las μ consideremos la descomposición (4.40) con $n \leftarrow i$. Dado que $p(-,-)$ es un mapeo bimultiplicativo, el producto de los últimos dos factores es precisamente $\mu_k^{m,i}$. En particular tenemos que

$$\mu_k^{m,i} = \sigma_k^m\left(\sigma_k^i\sigma_{i+1}^m\right)^{-1}. \tag{4.41}$$

Esta fórmula con (4.39) permite encontrar las μ. Concretamente, si $m < \psi(k)$, entonces

$$\mu_k^{m,i} = \begin{cases} q^{-4}, & \text{si } m > n,\ i = \psi(m) - 1; \\ 1, & \text{si } i = n; \\ q^{-2}, & \text{en otro caso.} \end{cases} \tag{4.42}$$

Si $m = \psi(k)$, esto es $x_m = x_k$, entonces

$$\mu_k^{m,i} = \begin{cases} q^2, & \text{si } i = n; \\ 1, & \text{en otro caso.} \end{cases} \tag{4.43}$$

Si $m > \psi(k)$, entonces las μ satisfacen $\mu_k^{m,i} = \mu_{\psi(m)}^{\psi(k),\psi(i)-1}$. Entonces es posible emplear (4.42):

$$\mu_k^{m,i} = \begin{cases} q^{-4}, & \text{si } k \leq n,\ i = \psi(k); \\ 1, & \text{si } i = n; \\ q^{-2}, & \text{en otro caso.} \end{cases} \tag{4.44}$$

Se definen los corchetes de $u(k,m)$, $k \leq m$ del siguiente modo

$$u[k,m] = \begin{cases} [[[\ldots[x_k, x_{k+1}], \ldots], x_{m-1}], x_m], & \text{si } m < \psi(k); \\ [x_k, [x_{k+1}, [\ldots, [x_{m-1}, x_m]]]], & \text{si } m > \psi(k); \\ \beta[u[n+1,m], u[k,n]], & \text{si } m = \psi(k), \end{cases} \tag{4.45}$$

donde $\beta = -p(u(n+1,m), u(k,n))^{-1}$, normaliza el coeficiente en $u(k,m)$. La identidad condicional (4.9) muestra que el valor de $u[k,m]$ en $U_q^+(\mathfrak{so}_{2n+1})$ es independiente de la alineación de corchetes dado que $m \leq n$ o $k > n$.

Con $\sim$ denotamos la igualdad proyectiva: $a \sim b$ si y sólo si $a = \alpha b$, donde $0 \neq \alpha \in \mathbf{k}$.

4.17 Lema. *Si $t \in \{k-1, k\}$, $t < n$, entonces $[u[k,n], x_t] = [x_t, u[k,n]] = 0$.*

Demostración. Si $t \leq k-2$, entonces la igualdad se sigue del segundo grupo de relaciones definitorias (4.13). Sea $k < t < n$. Por (4.8) podemos escribir

$$[u[k,n], x_t] = [[u[k,t-2], u[t-1,n]], x_t] = [u[k,t-2], [u[t-1,n], x_t]].$$

□

Por el Lema 4.14, el elemento $[u[t-1,n],x_t]$ es igual con cero en $U_{q^2}^+(\mathfrak{sl}_{n+1})$ dado que la palabra $u(t-1,n)x_t$ es estándar y los corchetes estándar son precisamente $[u[t-1,n],x_t]$. Este elemento es lineal en x_n. Por consiguiente, $[u[k,n],x_t]=0$ en $U_q^+(\mathfrak{so}_{2n+1})$ también gracias al Lema 4.13. Puesto que $p(u(k,n),x_t)\,p(x_t,u(k,n))=p_{tt+1}p_{tt}p_{tt-1}\cdot p_{t+1t}p_{tt}p_{t-1t}=1$, la identidad antisimétrica (4.14) puede aplicarse.

4.18 Lema. *Si $t\in\{\psi(m)-1,\psi(m)\}$, $t<n<m$, entonces*

$$[x_t,u[n+1,m]]=[u[n+1,m],x_t]=0.$$

Demostración. Si $t\leq\psi(m)-2$, entonces la relación requerida se sigue del segundo grupo de relaciones (4.13). Sea $\psi(m)<t<n$. Por el Lema 4.1 el valor de $u[n+1,m]$ en $U_q^+(\mathfrak{so}_{2n+1})$ es independiente de la alineación de los corchetes. En particular $u[n+1,m]=[[w,[x_{t+1}x_tx_{t-1}]],v]$, donde

$$w=u[n+1,\psi(t)-2],v=u[\psi(t)+2,m]$$

. Puesto que $p_{tt+1}p_{tt}p_{tt-1}\cdot p_{t+1t}p_{tt}p_{t-1t}=1$, la identidad antisimétrica (4.14) y la primera de (4.36) implican $[x_t,[x_{t+1}x_tx_{t-1}]]\sim[[x_{t-1}x_tx_{t-1}],x_t]=0$. Queda notar que $[x_t,w]=[w,x_t]=0$, $[x_t,v]=[v,x_t]=0$ de acuerdo con el segundo grupo de relaciones definitorias (4.13). □

4.19 Lema. *Si $k\leq n<m<\psi(k)$, entonces el valor en $U_q^+(\mathfrak{so}_{2n+1})$ de la palabra en corchetes $[y_kx_{n+1}x_{n+2}\dots x_m]$, donde $y_k=u[k,n]$, es independiente de la alineación particular de los corchetes.*

Demostración. Para aplicar (4.9) es suficiente con verificar $[u[k,n],x_t]=0$, $n+1<t\leq m$. Dado que la aplicación de ψ cambia el orden, tenemos que $k<\psi(m)\leq\psi(t)<n$. Por consiguiente, tomando en cuenta $x_t=x_{\psi(t)}$, es posible aplicar el Lema 4.17. □

4.20 Lema. *Si $k\leq n<\psi(k)<m$, entonces el valor en $U_q^+(\mathfrak{so}_{2n+1})$ de la palabra en corchetes $[x_kx_{k+1}\dots x_ny_m]$, donde $y_m=u[n+1,m]$, es independiente de la alineación particular que tengan los corchetes.*

Demostración. Para aplicar (4.9) es necesario $[x_t,u[n+1,m]]=0$, $k\leq t<n$. Para obtener dichas igualdades, se emplea el Lema 4.18. □

4.21 Lema. *Si $m\neq\psi(k)$, $k\leq i<n<m$, entonces*

$$[u[k,i],u[n+1,m]]=[u[n+1,m],u[k,i]]=0$$

a menos que $i=\psi(m)-1$.

Demostración. Denotemos por $u = u[k,i]$, $w = u[n+1,m]$. Las relaciones (4.30) y (4.31) implican que $p_{uw}p_{wu} = 1$. Por (4.14), tenemos que $[u,w] = -p_{uw}[w,v]$.

Si $\psi(m) < k$, entonces por el Lema 4.18 tenemos que $[x_t, u[n+1,m]] = 0$, $k \leq t \leq i$. En tal caso, $[u[k,i], u[n+1,m]] = 0$.

Supongamos que $\psi(m) > k$. Si $i < \psi(m) - 1$, entonces gracias al segundo grupo de relaciones definitorias (4.13) tenemos que $[x_t, u[n+1,m]] = 0$, $k \leq t \leq i$. Por lo tanto, $[u[k,i], u[n+1,m]] = 0$.

Sea $\psi(m) \leq i < n$. Si empleamos la notación $u_1 = u[k, \psi(m) - 2]$, $u_2 = u[\psi(m) - 1, i]$, entonces ciertamente $u = [u_1, u_2]$ a menos que $k = \psi(m) - 1$, $u = u_2$. Dado que $[u_1, w] = 0$, la identidad de Jacobi condicional (4.8) implica que en ambos casos se requiere verificar que $[u_2, w] = 0$.

Hagamos $u_3 = \left[x_{\psi(m)-1}, x_{\psi(m)}\right]$, $u_4 = u[\psi(m)+1, i]$. Entonces $u_2 = [u_3, u_4]$ a menos que $i = \psi(m)$, $u_2 = u_3$. Por el Lema 4.18 tenemos $[x_t, u[n+1,m]] = 0$ para toda t, $\psi(m) <$, $t < n$. En consecuencia, $[u_4, w] = 0$. Así, la identidad de Jacobi con $u \leftarrow u_3$, $v \leftarrow u_4$ muestra que es suficiente con probar que $[u_3, w] = 0$.

Pongamos $w_1 = u[n+1, m-2]$, $w_2 = [x_{m-1}, x_m]$. Entonces $w = [w_1, w_2]$ a menos que $m - 2 = n$, $w = w_2$ (recordemos que estamos considerando el caso $\psi(m) \leq i < n$, en particular $\psi(m) \leq n - 1$ y así $m \geq \psi(n-1) = n + 2$). Tenemos que $[u_3, w_1] = 0$. Por lo tanto, la identidad de Jacobi (4.6), con $u \leftarrow u_3$, $v \leftarrow w_1$, $w \leftarrow w_2$ muestra que es suficiente con obtener $[u_3, w_2] = 0$; esto es, $[[x_{t-1}, x_t], [x_{t+1}, x_t]] = 0$ con $t = \psi(m) < n$. Puesto que $[[x_{t-1}, x_t], x_t] = 0$ es una de las relaciones definitorias, la identidad condicional (4.8) implica que $[[x_{t-1}, x_t], [x_{t+1}, x_t]] = [[x_{t-1}x_t x_{t+1}], x_t]$. Queda aplicar la segunda relación de (4.36) para llegar al resultado deseado. □

4.22 Lema. *Si $m \neq \psi(k)$, $k \leq n < i < m$, entonces*

$$[u[k,n], u[i+1,m]] = [u[i+1,m], u[k,n]] = 0$$

a menos que $i = \psi(k)$.

Demostración. La prueba es similar a la demostración del lema anterior. Se basa en el Lema 4.17 y la segunda relación de (4.36) de igual forma en que el lema anterior se basa en el Lema 4.18 y la primera relación (4.36). □

4.23 Corolario. *Si $m \neq \psi(k)$, $k \leq n < m$, entonces en $U_q^+(\mathfrak{so}_{2n+1})$ tenemos que*

$$u[k,m] = [u[k,n], u[n+1,m]] = \beta[u[n+1,m], u[k,n]], \tag{4.46}$$

donde $\beta = -p\left(u\left(n+1,m\right),u\left(k,n\right)\right)^{-1}$.

Demostración. Consideremos la notación $u = u\left[k,n\right]$, $v = u\left[n+1,m\right]$. Las igualdades (4.42), (4.44) con $i = n$ muestran que $p_{uv}p_{vu} = \mu_k^{m,n} = 1$, dado que $m \neq \psi\left(k\right)$. Así, $\left[u,v\right] = uv - p_{uv}vu = -p_{uv}\left[v,u\right]$. Esto prueba la segunda igualdad. Para probar la primera debe aplicarse el Lema 4.19 si $m < \psi\left(k\right)$, y el Lema 4.20 en cualquier otro caso. □

4.24 Proposición. *Si* $m \neq \psi\left(k\right)$, *entonces en* $U_q^+\left(\mathfrak{so}_{2n+1}\right)$ *para cada* $i, k \leq i < m$ *tenemos*

$$\left[u\left[k,i\right],u\left[i+1,m\right]\right] = u\left[k,m\right]$$

con sólo dos posibles excepciones con $i = \psi\left(m\right) - 1$, *y* $i = \psi\left(k\right)$.

Demostración. Si $m \leq n$ o $k \geq n+1$, entonces la afirmación se sigue de (4.9). Así, podemos suponer que $m > n$.

Si $i = n$, el Corolario 4.23 implica la fórmula requerida.

Si $i > n$, entonces el Corolario 4.23 conduce a $u\left[k,i\right] = \left[u\left[k,n\right],u\left[n+1,i\right]\right]$, mientras que por el Lema 4.22 se tiene que $\left[u\left[k,n\right],u\left[i+1,m\right]\right] = 0$. Entonces, (4.8) implica

$$\left[\left[u\left[k,n\right],u\left[n+1,i\right]\right],u\left[i+1,m\right]\right] = \left[u\left[k,n\right],\left[u\left[n+1,i\right],u\left[i+1,m\right]\right]\right].$$

Ahora, (4.9) muestra que $\left[u\left[n+1,i\right],u\left[i+1,m\right]\right] = \left[u\left[n,m\right]\right]$, y nuevamente la fórmula requerida está implícita en el Corolario 4.23.

Si $i < n$, entonces el Corolario 4.23 conduce a $u\left[i+1,m\right] = \left[u\left[i+1,n\right],u\left[n+1,m\right]\right]$, en tanto que por el Lema 4.21 tenemos que $\left[u\left[k,i\right],u\left[n+1,m\right]\right] = 0$. Por consiguiente, (4.8) implica

$$\left[\left[u\left[k,i\right],\left[u\left[i+1,n\right],u\left[n+1,m\right]\right]\right]\right] = \left[\left[u\left[k,i\right],\left[u\left[i+1,n\right]\right],u\left[n+1,m\right]\right]\right].$$

Ahora, (4.9) muestra que $\left[u\left[k,i\right],u\left[i+1,n\right]\right] = u\left[k,n\right]$, y de nuevo el Corolario 4.23 implica la fórmula deseada. □

4.25 Proposición. *Si* $m \neq \psi\left(k\right)$, $k \leq i < j < m$, $m \neq \psi\left(i\right)$, $j \neq \psi\left(i\right) - 1$, $j \neq \psi\left(k\right)$, *entonces* $\left[u\left[k,i\right],u\left[j+1,m\right]\right] = 0$. *Si adicionalmente* $i \neq \psi\left(j\right) - 1$, *entonces* $\left[u\left[j+1,m\right],u\left[k,i\right]\right] = 0$.

Demostración. Si $m \leq n$ o $k > n$, entonces $u[k,i]$ y $u[j+1,m]$ están separadas por x_j, y por consiguiente la afirmación se sigue del Lema 4.12.

Si $k \leq n < i$, entonces por el Corolario 4.23 tenemos que $u[k,i] = [a,b]$ con $a = u[k,n]$, $b = u[n+1,i]$. El segundo grupo de relaciones (4.13) implica que $[b, u[j+1,m]] = 0$, mientras que el Lema 4.22 implica que $[a, u[j+1,m]] = 0$. Entonces, por (4.6) se tiene la relación requerida.

Si $j < n \leq m$, entonces nuevamente por el Corolario 4.23 tenemos que $u[j+1,m] = [a,b]$ con $a = u[j+1,n]$, $b = u[n+1,m]$. El segundo grupo de relaciones (4.13) implica que $[u[k,i], a] = 0$, mientras que el Lema 4.21 implica que $[u[k,i], b] = 0$. Entonces, por (4.6) se sigue la relación requerida.

Asumamos que $i \leq n \leq j$. Si $i > \psi(j) - 1$, entonces, tomando en cuenta el Lema 4.13, es posible aplicar el Lema 4.22 con $n \leftarrow i$, $i \leftarrow j$. De manera similar, si $i < \psi(j) - 1$, podemos emplear el Lema 4.21 con $n \leftarrow \psi(j) - 1$. Sea $i = \psi(j) - 1$. Podemos aplicar el caso $i > \psi(j) - 1$ a la secuencia $k \leq i < j' < m$ con $j' = j + 1$ a menos que $j' = m$, o $j' = \psi(k)$. Así, $[u[k,i], u[j+2,m]] = 0$, dado que $j+1 \neq m$, $j+1 \neq \psi(k)$. El Lema 4.1 implica que

$$[u[k,i], x_i] = [u[k,i-2], [[x_{i-1}, x_i], x_i]] = 0, \tag{4.47}$$

por la desigualdad $i < j - 1$ y la igualdad $i = \psi(j) - 1$ implica $i < n$. Ahora, si $j+1 \neq m$, $j+1 \neq \psi(k)$, entonces por el Lema 4.1 se tiene que

$$[u[k,i], u[j+1,m]] = [[u, [k,i], [x_i, u[j+2,m]]]] \overset{(4.8)}{=} [[u[k,i], x_i], u[j+2,m]] \overset{(4.47)}{=} 0,$$

para $x_{j+1} = x_i$. La igualdad excepcional $j + 1 = \psi(k)$ implica que $k = \psi(j) - 1 = i$. En este caso, por medio del Lema 4.1 tenemos

$$[x_i, u[j+1,m]] = [[x_i, [x_i, x_{i-1}]], u[j+3,m]] = 0.$$

Si en cambio $j + 1 = m$, entonces $u[1+j,m] = x_m = x_i$, para $\psi(j+1) = i$. Por consiguiente aplica la relación (4.47). La igualdad $[u[k,i], u[j+1,m]] = 0$ queda demostrada.

Asumamos que $i \neq \psi(j) - 1$. La definición de (4.38) muestra que

$$p(u(k,i), u(j+1,m)) \cdot p(u(j+1,m), u(k,i)) = \mu_k^{m,i} \left(\mu_k^{j,i}\right)^{-1}.$$

Usando (4.42) y (4.44) podemos probar que $\mu_k^{m,i} = \mu_k^{j,i}$. Si $i = n$, entonces $\mu_k^{m,i} = \mu_k^{j,i} = 1$. Sea $i \neq n$. Si $m < \psi(k)$, entonces $\mu_k^{m,i} = q^{-2}$, para $i = \psi(m) - 1$ es equivalente a $m = \psi(i) - 1$. De manera similar, $\mu_k^{j,i} = q^{-2}$, para $j \neq \psi(i) - 1$, y $j \leq m < \psi(k)$.

Si $m > \psi(k)$, e $i \neq \psi(k)$, entonces por (4.44) tenemos que $\mu_k^{m,i} = q^{-2}$, mientras que $\mu_k^{j,i} = q^{-2}$ en ambos casos: si $j < \psi(k)$ por (4.42), y si $j > \psi(k)$ por (4.44). Finalmente, si $i = \psi(k)$, entonces $j > i = \psi(k)$; por consiguiente (4.44) implica que $\mu_k^{m,i} = \mu_k^{j,i} = q^-$.

Para obtener $[u[j+1, m], u[k, i]] = 0$ resta aplicar (4.14). □

4.3. Generadores PBW del álgebra cuántica de Borel

4.26 Proposición. *Si $q^3 \neq 1$, $q^4 \neq 1$, entonces los valores de los elementos $u[k, m]$, $k \leq m < \psi(k)$ forman un conjunto de generadores PBW para el álgebra $U_q^+(\mathfrak{so}_{2n+1})$ sobre $\mathbf{k}[G]$ y todas las alturas son infinitas.*

Demostración. Por el Teorema B_n, el conjunto de generadores PBW (los valores de las súper letras duras en el Teorema 4.2) consiste en $[u_{km}]$, $k \leq m \leq n$, y $[w_{ks}]$, $1 \leq k < s \leq n$, donde $[u_{km}]$, $[w_{ks}]$ son precisamente las palabras $u(k, m)$, $u(k, \psi(s))$ con la alineación estándar de los corchetes. Por la identidad condicional (4.9) tenemos que $[u_{km}] = u[k, m]$ en $U_q^+(\mathfrak{so}_{2n+1})$. De acuerdo con A.8 los corchetes en $[w_{ks}]$ están definidos por las siguientes fórmulas de recurrencia:

$$\begin{aligned} [w_{ks}] &= [x_k [w_{k+1s}]], \text{ si } 1 \leq k < s-1; \\ [w_{kk+1}] &= [[w_{kk+2}] x_{k+1}], \text{ si } 1 \leq k < n, \end{aligned} \tag{4.48}$$

donde por definición $w_{kn+1} = u(k, n)$. Debemos verificar la igualdad $[w_{ks}] = u[k, \psi(s)]$ en $U_q^+(\mathfrak{so}_{2n+1})$. Si $k = n-1$, $s = n$, entonces $w_{ks} = [[x_{n-1}, x_n], x_n] = u[n-1, n+2]$.

Si $k < s-1$, entonces por (4.8) tenemos

$$[x_k, [u[k+1, n], u[n+1, \psi(s)]]] = [u[k, n], u[n+1, \psi(s)]],$$

para $[x_k, x_t] = 0$, $n+1 \leq t \leq \psi(s)$. Así, es posible aplicar inducción gracias a (4.46).

Si $s = k+1 < n$, entonces la segunda opción de (4.48) se cumple. Esto permite aplicar la igualdad recién probada para $[w_{kk+2}]$. □

Si q no es una raíz de 1, entonces la cuarta afirmación del Teorema B_n muestra que cada elemento primitivo torcido en $U_q^+(\mathfrak{so}_{2n+1})$ es proporcional a cualquier x_i, $1 \leq i \leq n$, o $1-g$, $g \in G$. En particular, $\epsilon\left(G\langle X\rangle^{(2)}\right)$ no tiene elementos primitivos torcidos distintos de cero. Al mismo tiempo, gracias al Teorema de Heyneman-Radford [24], [36, Corolario 5.3], todo biideal de una álgebra de Hopf caracter tiene elementos primitivos torcidos distintos de cero. Por lo tanto, $\ker \epsilon = \mathbf{\Lambda}$, mientras que la subálgebra A generada por los valores de x_i, $1 \leq i \leq n$ en $U_q^+(\mathfrak{so}_{2n+1})$ tiene la representación barajada.

Si el orden multiplicativo de q es finito, entonces por la definición de $H = u_q^+(\mathfrak{so}_{2n+1})$ tenemos que $\ker \epsilon = \mathbf{\Lambda}$. Por lo tanto, la subálgebra A generada por los valores de x_i, $1 \leq i \leq n$ en $u_q^+(\mathfrak{so}_{2n+1})$ tiene también una representación barajada.

Recordemos que por $(u,(m,k))$ denotamos al tensor $x_m \otimes x_{m-1} \otimes \ldots \otimes x_k$ considerado como elemento de $Sh_\tau(V)$.

4.27 Proposición. *Sea $k \leq m \leq 2n$. En la representación barajada tenemos*

$$u[k,m] = \alpha_k^m \cdot (u(m,k)), \qquad \alpha_k^m \stackrel{\text{def}}{=} \epsilon_k^m (q2-1)^{m-k} \cdot \prod_{k \leq i < j \leq m} p_{ij}, \tag{4.49}$$

donde

$$\epsilon_k^m = \begin{cases} 1, & \text{si } m \leq n \text{ o } k > n; \\ q^{-1}, & \text{si } k \leq n < m,\ m \neq \psi(k); \\ q^{-3}, & \text{si } m = \psi(k). \end{cases} \tag{4.50}$$

Demostración. Emplearemos inducción en $m-k$. Si $m = k$, la igualdad se reduce a $x_k = (x_k)$.

i) Consideremos primero el caso $m < \psi(k)$. Por la hipótesis inductiva tenemos que $u[k,m-1] = \alpha_k^{m-1} \cdot (w)$, $w = u(m-1,k)$. Al usar (4.21) podemos escribir

$$\begin{aligned} u[k,m] &= \alpha_k^{m-1} \{(w)(x_m) - p(w,x_m) \cdot (x_m)(w)\} \\ &= \alpha_k^{m-1} \sum_{uv=w} \left\{p(x_m,v)^{-1} - p(w,x_m)\, p(u,x_m)^{-1}\right\} (ux_mv). \end{aligned} \tag{4.51}$$

Puesto que $w = uv$, tenemos que $p(w, x_m)\, p(u, x_m)^{-1} = p(v, x_m)$.

Si $m \leq n$, entonces las relaciones (4.31) implican que $p(v, x_m)\, p(x_m, v) = 1$ con sólo una excepción: $v = w$. Por consiguiente, la suma (4.60) tiene sólo un término. El coeficiente en $(x_m w) = (u(m, k))$ es igual con

$$\alpha_k^{m-1} p(w, x_m) \left(p(w, x_m)^{-1} p(x_m, w)^{-1} - 1 \right) = \alpha_k^{m-1} p(w, x_m) \left(q^2 - 1 \right),$$

como se requiere.

Si $m = n + 1$, entonces aún $p(v, x_m)\, p(x_m, v) = 1$ con dos excepciones: $v = w$ y $v = u(n - 1, k)$. En ambos casos $(u x_m v)$ es igual con $(u(m, k))$. En consecuencia el coeficiente de $(u(m, k))$ en la suma (4.60) es igual a

$$p(x_n, u(k, n-1))^{-1} - p(u(k, n-1), x_n) + p(x_n, u(k, n))^{-1} - p(u(k, n), x_n),$$

es decir,

$$p(w, x_{n+1}) \left\{ p_{nn-1}^{-1} p_{n-1n}^{-1} p_{nn}^{-1} - p_{nn}^{-1} + p_{nn-1}^{-1} p_{nn}^{-1} p_{nn}^{-1} p_{n-1n}^{-1} - 1 \right\}.$$

Por (4.30) y (4.31) tenemos que $\alpha_k^m = \alpha_k^{m-1} p(w, x_{n+1}) (q^2 - 1) q^{-1}$.

Supongamos que $m > n + 1$. En este caso, por la definición de $x_m = x_t$, donde $t = \psi(m) < \psi(n + 1) = n$. Sea $v = u(s, k)$. Si $s < t - 1$, entonces v depende sólo de x_i, $i < t - 1$, y las relaciones (4.30) y (4.31) implican que $p(v, x_m)\, p(x_m, v) = 1$. si $s > t$, $s \neq m - 1$, entonces $p(v, x_m)\, p(x_m, v) = p_{t-1} p_{tt} p_{t+1t} \cdot p_{tt-1} p_{tt} p_{t+1t} = 1$. Por lo tanto, en (4.60) quedan tres términos con $s = t - 1$, $s = t$ y $s = m - 1$. Si $v = u(t - 1, k)$ o $v = u(t, k)$, entonces $(u x_m v)$ es igual a $(u(k, t)\, x_t^2\, u(t + 1, m - 1))$, en tanto que el coeficiente del tensor en la suma (4.60) es

$$p(x_t, u(k, t-1))^{-1} - p(u(k, t-1), x_t) + p(x_t, u(k, t))^{-1} - p(u(k, t), x_t)$$

esto es,

$$p(u(k, t), x_t) \left\{ p_{tt-1} - 1 p_{t-1}^{-1} p_{tt}^{-1} - p_{tt}^{-1} + p_{tt}^{-1} p_{tt-1}^{-1} p_{t-1t}^{-1} p_{tt}^{-1} - 1 \right\} = 0.$$

Así, en (4.60) resta un término con $v = u(m - 1, k)$. Éste tiene el coeficiente requerido:

$$\alpha_k^m = \alpha_k^{m-1} \left(p(x_m, w)^{-1} - p(w, x_m) \right) = \alpha_k^{m-1} p(w, x_m) \left(q^2 - 1 \right). \tag{4.52}$$

ii) De forma análoga, consideremos el caso en el que $m > \psi(k)$. Por la hipótesis inductiva, tenemos que $u[k + 1, m] = \alpha_{k+1}^m \cdot (w)$, $w = u(m, k + 1)$. Empleando (4.21) podemos

escribir

$$\begin{aligned} u[k,m] &= \alpha_{k+1}^{m} \left\{ (x_k)(w) - p(x_k,w) \cdot (w)(x_k) \right\} \\ &= \alpha_{k+1}^{m} \sum_{uv=w} \left\{ p(u,x_k)^{-1} - p(x_k,u) \right\} (ux_kv). \end{aligned} \tag{4.53}$$

Si $k > n$, entonces $p(u,x_k)\,p(x_k,u) = 1$, a menos que $u = w$. Así, (4.53) tiene solamente un término, y el coeficiente es igual con

$$\alpha_{k+1}^{m} p(x_k,w) \left(p(w,x_k)^{-1} p(x_k,w)^{-1} - 1 \right) = \alpha_{k+1}^{m} p(x_k,w) \left(q^2 - 1 \right),$$

como se requería.

Si $k = n$, entonces $p(u,x_k)\,p(x_k,u) = 1$ con dos excepciones: $u = w$ y $u = u(m,n+2)$. En ambos casos (ux_kv) es igual con $(u(m,k))$, mientras que el coeficiente toma la forma

$$p(w,x_n)^{-1} - p(x_n,w) + p(u(m,n+2),x_n)^{-1} - p(x_n,u(m,n+2))$$

que es igual con

$$p(x_n,w) \left\{ p_{nn-1}^{-1} p_{n-1n}^{-1} p_{nn}^{-2} - 1 + p_{nn-1}^{-1} p_{n-1n}^{-1} p_{nn}^{-1} - p_{nn}^{-1} \right\}.$$

Gracias a las relaciones (4.30), (4.31) se tiene que $\alpha_n^m = \alpha_{n+1}^m p(x_n,w)\,(q^2-1)\,q^{-1}$, como se buscaba.

Supongamos que $k < n$. En este caso, $x_k = x_t$ con $m > t \overset{\text{def}}{=} \psi(k) > \psi(n) = n+1$. Sea $u = u(m,s)$. Si $s > t$, entonces u depende sólo de x_i, $i < k-1$, y las relaciones (4.30), (4.31) implican que $p(x_k,u)\,p(u,x_k) = 1$. Si $s < t-1$, $s \neq k+1$, entonces $p(x_k,u)\,p(u,x_k) = p_{k-1k}p_{kk}p_{k+1k} \cdot p_{kk-1}p_{kk}p_{k+1k} = 1$. De manera que en (4.53) quedan tres términos con $s = t$, $s = t+1$, y $s = k+1$. Si $u = u(m,t)$ o $u = u(m,t+1)$, entonces $ux_kv = u(m,t+1)\,x_k^2 u(t-1,k)$, en tanto que el coeficiente del tensor correspondiente es

$$p(u(m,t+1),x_k)^{-1} - p(x_k,u(m,t+1)) + p(u(m,t),x_k)^{-1} - p(x_k,u(m,t)),$$

es decir,

$$p(x_k,u(m,t+1)) \left\{ p_{k-1k}^{-1} p_{kk-1}^{-1} - 1 + p_{kk}^{-1} p_{k-1k}^{-1} p_{kk-1}^{-1} - p_{kk} \right\} = 0.$$

Así, en (4.60) queda un sólo término, y

$$\alpha_k^m = \alpha_{k+1}^m \left(p(w,x_k)^1 - p(x_k,w) \right) = \alpha_{k+1}^m p(x_k,w) \left(q^2 - 1 \right).$$

iii) Consideremos el caso faltante en el que $m = \psi(k)$. En este caso $x_m = xk$. Si $k = n$, $m = n+1$, entonces $u[n, n+1] = -p_{nn}^{-1}[x_n, x_n] = (1-q^{-1})x_n^2$, mientras que en la representación barajada tenemos $(x_n)(x_n) = (1+q^{-1})(1+q^{-1})(x_n x_n)$. Entonces, $u[n, n+1] = (1-q^{-2})(x_{n+1}x_n)$, lo cual se requiere: $(1-q^{-2}) = q^{-3}\cdot(q^2-1)\cdot p_{nn}$.

Si $k < n$, hacemos $u[n+1, m]$, $v = x_k$, $w = u[k+1, n]$. Por la definición de (4.45) se sigue que $u[k, m] = \beta[u, [v, m]]$, donde $\beta = -p(u(n+1, m), u(k, n))^{-1}$; esto es, $\beta = -p_{u,vw}^{-1}$. En virtud de que $u[n+1, m] = [u[n+1, m-2], [x_{k+1}, x_k]]$, la identidad condicional (4.8) implica que $[u, v] = [u[n+1, m-2], [[x_{k+1}, x_k], x_k]] = 0$. Así, $[[u, v], w] = 0$, y la fórmula (4.7) conduce a

$$\beta^{-1}u[k, m] = p_{uv}x_k \cdot [u, w] - p_{vu}[u, w]\cdot x_k. \tag{4.54}$$

La fórmula (4.46) implica que $\beta_1[u, w] = u[k+1, m]$ con $\beta_1 = -p_{uw}^{-1}$. Por consiguiente el caso anterior, el ii), nos permite encontrar la representación barajada $[u, w] = \alpha\cdot(z)$ con $z = u(m, k+1)$, y $\alpha = -p_{uw}\alpha_{k+1}^m$. Por (4.21) la representación barajada del lado derecho de (4.54) es

$$\alpha \sum_{sy=u(m,k+1)} \left(p_{uv}p(s, x_k)^{-1} - p_{vw}p(x_k, y)^{-1}\right)\cdot(sx_k y).$$

Tenemos que $\beta_\alpha = \beta p_{uw}\alpha_{k+1}^m = p_{uv}^{-1}\alpha_{k+1}^m$, y

$$p_{uv}p_{vu} = p_{k+1k}p_{kk}p_{kk+1}p_{kk} = q^2$$

dado que $k < n$. Por lo tanto, se sigue que

$$u[k, m] = \alpha_{k+1}^m \sum_{sy=u(m,k+1)} \left(p(s, x_k)^{-1} - q^2 p(x_k, s)\right)\cdot(sx_k y). \tag{4.55}$$

Si $s \notin \{\emptyset, x_m, z = u(m, k+1)\}$, entonces $p(s, x_k)p(x_k, s) = p_{k+1}p_{kk}p_{kk+1}p_{kk} = q^2$, que como en (4.55) sigue teniendo sólo tres elementos. Si $s \neq \emptyset$ o $s = x_m$, entonces $(sx_k y) = (x_k z)$ dado que $x_m = x_k$. En consecuencia, el coeficiente en $(x_k z)$ en (4.55) es igual con $1 - q^2 + p_{kk}^{-1} - q^{-2}p_{kk} = 0$. Así, en (4.55) queda sólo un término con coeficiente

$$\alpha_{k+1}^m\left(p(z, x_k)^{-1} - q^{-2}p(x_k, z)\right) = \alpha_{k+1}^m p(x_k, z)\, q^{-2}\left(q^2-1\right) = \alpha_k^m$$

ya que $p(z, x_k)\cdot p(x_k, z) = p_{kk}p_{k+1k}p_{k+1k}\cdot p_{kk}p_{kk+1}p_{kk+1} = 1$. □

4.28 Teorema. *En $U_q^+(\mathfrak{so}_{2n+1})$ el coproducto en los elementos $u[k, m]$, $k \le m \le 2n$ tiene la siguiente forma explícita:*

$$\begin{aligned}\Delta(u[k, m]) =& u[k, m]\otimes 1 + g_k g_{k+1}\ldots g_m \otimes u[k, m] \\ &+ \sum_{i=k}^{m-1} \tau_i\left(1-q^{-2}\right) g_k g_{k+1}\ldots g_i u[i+1, m]\otimes u[k, i],\end{aligned} \tag{4.56}$$

donde $\tau_i = 1$ *con sólo una excepción;* $\tau_n = q$.

Demostración. Las fórmulas (4.49), (4.20) y (4.19) muestran que el coproducto tiene la forma (4.56), donde $\tau_i\left(1-q^{-2}\right) = \alpha_k^m \left(\alpha_k^i \alpha_{i+1}^m\right)^{-1} \chi^{u(i+1,m)}\left(g_k g_{k+1} \dots g_i\right)$. Tenemos

$$\left(\prod_{k\le a<b\le i} p_{ab} \prod_{i+1\le a<b\le m} p_{ab}\right)^{-1} \prod_{k\le a<b\le m} p_{ab} = p\left(u\left(k,i\right), u\left(i+1\right), m\right).$$

Por lo tanto, la definición de μ_k^m dada en (4.38) y la definición de α_k^m dada en (4.49) implica que $\tau_i\left(1-q^{-2}\right) = \epsilon_k^m \left(\epsilon_k^i \epsilon_{i+1}^m\right)^{-1}\left(q^2-1\right)\mu_k^{m,i}$; esto es, $\tau_i = \epsilon_k^m \left(\epsilon_k^i \epsilon_{i+1}^m\right)^{-1} q^2 \mu_k^{m,i}$. Por (4.41) tenemos que $\mu_k^{m,i} = \sigma_k^m \left(\sigma_k^i \sigma_{i+1}^m\right)^{-1}$. Empleando (4.39) y (4.50) se observa que

$$\epsilon_k^m \sigma_k^m = \begin{cases} q^2, & \text{si } m < n \text{ o } k > n+1; \\ q, & \text{en otro caso.} \end{cases} \tag{4.57}$$

Ahora las τ tienen la siguiente forma elegante

$$\tau_i = \epsilon_k^m \sigma_k^m \left(\epsilon_k^i \sigma_k^i\right)^{-1} \left(\epsilon_{i+1}^m \sigma_{i+1}^m\right)^{-1} q^2 = \begin{cases} q, & \text{si } i = n; \\ 1, & \text{en otro caso.} \end{cases} \tag{4.58}$$

Es interesante notar que la fórmula del coproducto difiere de la de $U_{q^2}^+\left(\mathfrak{sl}_{2n+1}\right)$ por tan sólo un término (véase fórmula (3.3) en [42]). □

Ahora, hallaremos los generadores PBW de $u_q^+\left(\mathfrak{so}_{2n+1}\right)$. Para ello requeriremos algunas relaciones adicionales en $U_q^+\left(\mathfrak{so}_{2n+1}\right)$.

4.29 Lema. *Si* $k \le m < \psi\left(k\right)$*, entonces en el álgebra* $U_q^+\left(\mathfrak{so}_{2n+1}\right)$ *se tiene que*

$$\left[u\left[k,m\right], \left[u\left[k,m\right], u\left[k+1,m\right]\right]\right] = 0. \tag{4.59}$$

Demostración. Primero, supongamos que $m < \psi\left(k\right) - 1$. En tal caso, tanto $u\left(k,m\right)$ como $u\left(k+1,m\right)$ son estándar. La alineación estándar de corchetes de estas palabras se define por (4.48). Sin embargo, en la Proposición 4.26 hemos visto que $\left[u\left(k,m\right)\right] = u\left[k,m\right]$, y por consiguiente también $\left[u\left(k+1,m\right)\right] = u\left[k+1,m\right]$ en el álgebra $U_q^+\left(\mathfrak{so}_{2n+1}\right)$.

La palabra $w = u\left(k,m\right) u\left(k,m\right) u\left(k+1,m\right)$ es estándar. El algoritmo expuesto al inicio del capítulo muestra que la alineación estándar de corchetes es precisamente

$$\left[\left[u\left(k,m\right)\right], \left[\left[u\left(k,m\right)\right], \left[u\left(k+1,m\right)\right]\right]\right]. \tag{4.60}$$

De modo que la súper palabra $[w]$ en $U_q^+(\mathfrak{so}_{2n+1})$ es igual al lado izquierdo de (4.59).

Por la Proposición 4.26 todas las súper letras duras en $U_q^+(\mathfrak{so}_{2n+1})$ son $[u(k,m)]$, $k \leq m < \psi(k)$. Así, $[w]$ no es dura. El uso múltiple de la Definición 3.14 muestra que el valor de $[w]$ es una combinación lineal de valores de súper palabras en menos de $[w]$ súper letras duras. Puesto que $U_q^+(\mathfrak{so}_{2n+1})$ es homogénea, cada una de las súper palabras en esa descomposición tiene dos súper letras duras menores que $[w]$ y de grado 1 en x_k (si una súper letra dura $[u(r,s)]$ es de grado 2 en x_k, entonces $r < k$ y $u(r,s) > w$). Al mismo tiempo todas esas súper letras duras son $[u(k,m+1)], [u(k,m+2)], \ldots, [u(k,2n-k)]$. Cada uno de ellos tiene grado 2 en x_{m+1} si $m \geq n$, y al menos 1 si $m < n$. Entonces, la súper palabra tiene grado al menos 4 en x_{m+1} si $m \geq n$, y al menos 1 si $m < n$. Sin embargo, w es de grado 3 en x_{m+1} si $m \geq n$, y es independiente de x_{m+1} si $m < n$. Por lo tanto, la descomposición es vacía, y $[w] = 0$.

Sea, entonces, $m = \psi(k) - 1$. En este caso, $u(k+1,m)$ no es estándar y por esa razón no es posible aplicar los argumentos previos. A pesar de ello, podemos probar de forma similar que $[u[k,2n-k], x_t] = 0$, $k < t \leq n$. Esto implicaría que $[u[k,2n-k], u[k+1,2n-k]] = 0$ y (4.59).

Si $k+1 < t < n$, entonces por el Lema 4.17 y el Lema 4.18:

$$[u[k,n], x_t] = [u[n+1,2n-k], x_t] = 0.$$

Por medio del Corolario 4.23 tenemos que $[u[k,2n-k], x_t] = 0$.

Si $t = k+1$, consideremos la palabra $v = u(k,2n-k)x_{k+1}$. Esta es una palabra estándar, y la alineación estándar de corchetes es $[v] = [[u(k,2n-k)]x_{k+1}]$. Por lo tanto, el valor de la súper letra $[v]$ es igual con $[u[k,2n-k], x_{k+1}]$. Al mismo tiempo $[v]$ no pertenece al conjunto de generadores PBW; esto es, no es dura. El uso múltiple de la Definición 3.14 muestra que el valor de $[v]$ es una combinación lineal de valores de súper palabras menores en $[v]$ súper letras duras. Cada una de las súper palabras en dicha descomposición tiene una súper letra dura menor que $[v]$ y de grado 1 en x_k. Sin embargo, no hay tales súper letras. Así, la descomposición es vacía y $[v] = 0$.

Sea $t = n$. Si $k = n-1$, entonces $[u[k,2n-k], x_n] = [[[x_{n-1}, x_n], x_n], x_n] = 0$ debido a (4.33). Si $k = n-2$, consideramos a la palabra $u = u(k,2n-k)x_n = x_{n-2}x_{n-1}x_nx_nx_{n-1}x_n$. Esta es una palabra estándar, mientras que la súper letra $[u]$ no lo es. De nuevo, no existe una súper letra dura menor que $[u]$ y de grado 1 en

x_{n-2}. Por consiguiente $[u] = 0$ en $U_q^+(\mathfrak{so}_{2n+1})$. La alineación estándar de corchetes es $[[x_{n-2}x_{n-1}x_nx_n]\,[x_{n-1}x_n]]$. Por lo tanto, tenemos que

$$[[x_{n-2}, [[x_{n-1}, x_n], x_n]], [x_{n-1}, x_n]] = 0.$$

Al mismo tiempo $[x_{n-2}] = 0$ y $[[[x_{n-1}, x_n], x_n], x_n] = 0$ implica que

$$[[x_{n-2}, [[x_{n-1}, x_n], x_n]], x_n] = 0.$$

La identidad condicional (4.8) conduce a

$$[[x_{n-2}, [[x_{n-1}, x_n], x_n]], [x_{n-1}, x_n]] = [[[x_{n-2}, [[x_{n-1}, x_n], x_n]], x_{n-1}], x_n],$$

lo cual es requerido para $[u\,[n-2, n+2], x_n] = [[[x_{n-2}, [[x_{n-1}, x_n], x_n]], x_{n-1}], x_n]$.

Finalmente, supongamos que $k < n-2$. Emplearemos la notación $u_1 = u\,[k, n-3]$, $v_1 = u\,[n+3, 2n-k]$, $w_1 = u\,[n-2, n+2]$. Ya hemos probado que $[w_1, x_n] = 0$. El segundo grupo de relaciones (4.13) implica que $[u_1, x_n] = 0$, $[v_1, x_n] = 0$. Al mismo tiempo, por medio de la Proposición 4.24, tenemos que $u\,[k, 2n-k] = [u\,[k, n+2], v_1]$ y $u\,[k, n+2] = [u_1, w_1]$; que es $u\,[k, 2n-k] = [[u_1, w_1], v_1]$. Esto ciertamente implica la relación requerida $[u\,[k, 2n-k], x_n] = 0$. □

4.30 Proposición. *Si el orden multiplicativo t de q es finito, $t > 4$, entonces los valores de $u\,[k, m]$, $k \le m < \psi(k)$ forman un conjunto de generadores PBW para $u_q^+(\mathfrak{so}_{2n+1})$ sobre $\mathbf{k}[G]$. La altura h de $u\,[k, m]$ es igual con t si $m = n$ o t es impar. Si $m \ne n$ y t es par, entonces $h = t/2$. En todos los casos $u\,[k, m]^h = 0$ en $u_q^+(\mathfrak{so}_{2n+1})$.*

Demostración. Primero, notemos que la Definición 3.14 implica que la súper letra no dura en $U_q^+(\mathfrak{so}_{2n+1})$ es aún no dura en $u_q^+(\mathfrak{so}_{2n+1})$. Por lo tanto, todas las súper letras duras en $u_q^+(\mathfrak{so}_{2n+1})$ están en la lista $u\,[k, m]$, $k \le m < \psi(k)$. Si, luego, $u\,[k, m]$ no es dura en $u_q^+(\mathfrak{so}_{2n+1})$, entonces por el uso múltiple de la Definición 3.14 el valor de $u\,[k, m]$ es una combinación lineal de súper palabras en súper letras duras menores que $u\,[k, m]$. Puesto que $u_q^+(\mathfrak{so}_{2n+1})$ es homogénea, cada una de las súper palabras en dicha descomposición tiene una súper letra dura menor que $u\,[k, m]$ y de grado 1 en x_k. Al mismo tiempo todas las súper letras duras están en la lista $[u\,(k, m+1)], [u\,(k, m+2)], \ldots, [u\,(k, 2n-k)]$. Cada una de ellas tiene grado 2 en x_{m+1} si $m \ge n$, y al menos 1 si $m < n$. Por consiguiente la súper palabra tiene grado al menos 2 si $m \ge n$, y al menos 1 si $m < n$. Sin embargo, $u\,[k, m]$ es de grado 1 en x_{m+1} si $m \ge n$, y es independiente de x_{m+1} si $m < n$. Por lo tanto, la descomposición es vacía, y $u\,[k, m] = 0$. Esto contradice a la Proposición 4.27, por $(u\,(m, k)) \ne 0$ en el álgebra barajada.

Para simplificar la notación, emplearemos ahora la notación $u = u\,[k, m]$. La ecuación (4.39) implica que $p_{uu} = q$ si $m = n$ y $p_{uu} = q^2$ en otro caso (recordemos que ahora $m <$

$\psi(k)$). Por la Definición 3.16 el valor mínimo posible para las alturas es precisamente la h dada en la proposición. Queda probar que $u^h = 0$ en $u_q^+(\mathfrak{so}_{2n+1})$. Por el Lema 4.8 es suficiente con demostrar que $\partial_i\left(u^h\right) = 0$, $1 \leq i \leq n$. El Lema 4.7 conduce a

$$\partial_i\left(u^h\right) = p(u, x_i)^{h-1} \underbrace{[u, [u, \ldots [u}_{h-1}\ , \partial_i(u)] \ldots]] .$$

La fórmula del coproducto (4.56) con (4.23) implica que

$$\partial_i(u) = \begin{cases} (1 - q^{-2})\, \tau_k u\,[k+1, m]\,, & \text{si } i = k < m; \\ 0, & \text{si } i \neq k; \\ 1, & \text{si } i = k = m. \end{cases} \tag{4.61}$$

Al mismo tiempo el Lema 4.29 brinda la relación $[u, [u, u\,[k+1, m]]] = 0$ en $U_q+(\mathfrak{so}_{2n+1})$, y por consiguiente también en $u_q^+(\mathfrak{so}_{2n+1})$. Dado que siempre $h > 2$, tenemos las igualdades requeridas $\partial_i\left(u^h\right)$, $1 \leq i \leq n$. □

Para probar (4.56) empleamos la representación barajada. Por lo tanto, si q tiene un orden multiplicativo finito, entonces (4.56) está demostrado sólo para $u_q^+(\mathfrak{so}_{2n+1})$. Sin embargo hemos visto que el kernel del homomorfismo natural $U_q^+(\mathfrak{so}_{2n+1}) \to u_q^+(\mathfrak{so}_{2n+1})$ es generado por los elementos $u\,[k, m]^h$, $k \leq m < \psi(k)$. El grado de $u\,[k, m]^h$ en una x_i dada es cero o mayor que 2. Al mismo tiempo, todos los tensores en (4.56) tienen grado menor o igual a 2 en cada variable. Por lo tanto, (4.56), y en consecuencia (4.61) son válidas en $U_q^+(\mathfrak{so}_{2n+1})$ dado que q también tiene un orden multiplicativo finito $t > 4$.

Capítulo 5

Rango combinatorio de $u_q(\mathfrak{so}_{2n+1})$

Como se expuso en la introducción del presente trabajo, los anillos finitos juegan un papel importante en la Teoría de Códigos. Para comprender la relación entre los códigos, los anillos finitos de Frobenius y los grupos cuánticos, la extensión del teorema de MacWilliams resulta fundamental. Este teorema, aborda la noción de equivalencia entre códigos: dos códigos son equivalentes si existe una transformación monomial que lleve del primero, al segundo. Esta descripción extrínseca tiene la siguiente formulación intrínseca: si dos códigos son isomórficos como espacios vectoriales abstractos a través de un isomorfismo que preserve el peso de Hamming, entonces este isomorfismo se extiende a una transformación monomial.

El problema de extensión original plantea la siguiente pregunta: siendo $n \in \mathbb{Z}^+$, $C \subseteq R^n$ un código lineal sobre un campo R con $C \subseteq R^n$, y $f : C \to R^n$ una isometría lineal, ¿existe una isometría lineal (una transformación monomial) $T : R^n \to R^n$ tal que T restringida a C_1 se igual a f? MacWilliams mostró que, cuando R es un campo finito, este problema siempre tiene solución. Dicho resultado se conoce como el Teorema de equivalencia de MacWilliams, pero también como la Extensión del teorema de MacWilliams debido a su similitud con las extensiones de los teorema de Witt y Art para formas bilineales y cuadráticas (véase [17]).

Por otra parte, recordemos que el peso de Hamming se define como el número de coordenadas distintas de cero en una palabra de código. Se dice que un anillo finito R tiene la propiedad de extensión para el peso de Hamming si existe la citada isometría lineal. La Extensión del teorema de MacWilliams fue probada por Wood en [76] sobre anillos de Frobenius finitos.

En otras palabras, el teorema establece que todo anillo de Frobenius finito tiene la propiedad de extensión para el peso de Hamming.

El inverso de este resultado, también probado por Wood en [75], se verifica: todo anillo finito que tiene la propiedad de extensión para el peso de Hamming es de Frobenius. Esto sugiere que los anillos de Frobenius finitos son la clase más apropiada de anillos para la Teoría de Códigos. Por ello, el estudio de códigos sobre anillos de Frobenius finitos resulta de gran interés.

La relación de estos resultados con la teoría de los grupos cuánticos se desprende del hecho de que toda álgebra de Hopf finita es de Frobenius, probado por Larson en [47]. Por supuesto, debido a la Extensión del teorema de MacWilliams, las álgebras de dimensión finita sobre campos son de gran interés para la Teoría de Códigos, pues éstas son anillos de Frobenius. De esta forma, los grupos finitos cuánticos proveen un campo fértil para trabajar con ellos en el contexto de la Teoría de Códigos.

En el contexto de los grupos cuánticos, el teorema fundamental de Heyneman-Radford afirma que un morfismo de coálgebras es inyectivo siempre que su restricción sobre el primer componente de la filtración coradical sea inyectiva. Al aplicar esto a morfismos de biálgebras (o álgebras trenzadas), tenemos que los biideales distintos de cero tienen intersecciones distintas de cero con el primer componente de la filtración coradical. En el caso particular de las biálgebras coconmutativas conectadas, cada biideal es incluso generado como un ideal en dicha intersección. Esto no se verifica para una biálgebra no conmutativa arbitraria (un grupo cuántico) $\mathfrak{U}$. El teorema de Heyneman-Radford permite a sólo un biideal K de $\mathfrak{U}$ definir la secuencia de biideales $0 = J_0 \subset J_1 \subset J_2 \subset \ldots \subset J_i \subset \ldots$ tales que J_{i+1}/J_i como ideal es generado por la intersección con el primer componente de la filtración del coradical de $\mathfrak{U}/J_i$, y $K = \bigcup_i J_i$. La longitud de dicha secuencia es una característica importante de los homomorfismos φ con el kernel K.

En particular, si se obtiene una representación combinatoria sobre el coradical de la biálgebra $\mathfrak{U}$ por medio de los generadores y las relaciones $\varphi : H\langle X\rangle \to \mathfrak{U}$, entonces, por definición, el *rango combinatorio* de la biálgebra $\mathfrak{U}$ es la longitud de la secuencia anterior para el ker φ.

Para emplear una álgebra de Frobenius como alfabeto de un código en la práctica es preciso introducir esta álgebra en una computadora. El número de pasos necesarios para las representaciones combinatorias ordinarias es precisamente el rango combinatorio, por lo que éste es de particular interés en nuestro estudio.

En este capítulo, se muestra que el rango combinatorio de la versión multiparamétrica del grupo cuántico de Lusztig pequeño $u_q(\mathfrak{so}_{2n+1})$ de tipo B_n [55] es igual a $\lfloor \log_2(n-1) \rfloor + 2$ siempre que q tenga un orden finito multiplicativo $t > 4$. Por Kharchenko y Andrade [42] se sabe que el rango combinatorio de la versión multiparamétrica del kernel de Frobenius Lusztig de tipo A_n es igual a $\lfloor \log_2 n \rfloor + 1$.

5.1. Representación combinatoria

A continuación se explicará la representación combinatoria de los kernels de Frobenius-Lusztig.

Los grupos cuánticos $u_q(\mathfrak{so}_{2n+1})$, $U_q(\mathfrak{so}_{2n+1})$ son generados como $\mathbf{k}$-álgebras por medio de elementos de grupo $g_1, g_2, \ldots, g_n$, $f_1, f_2, \ldots, f_n$, $\Delta(g_i) = g_i \otimes g_i$, $\Delta(f_i) = f_i \otimes f_i$, sus inversos y elementos primitivos, $x_1, x_2, \ldots, x_n$, $x_1^-, x_2^{-1}, \ldots, x_n^-$,

$$\Delta(x_i) = x_i \otimes 1 + g_i \otimes x_i;\ \Delta(x_i^-) = x_i^- \otimes 1 + f_i \otimes x_i^-.$$

Todos los elementos en el grupo conmutan unos con otros, mientras que los generadores primitivos torcidos conmutan de esta forma:

$$x_i g_j = p_{ij} g_j x_i,\ x_i^- g_j = p_{ij}^{-1} g_j x_i^-,\ x_i f_j = p_{ji} f_j x_i, x_i^- f_j = p_{ji}^{-1} f_j x_i^-,$$

donde p_{ij} son parámetros arbitrarios que satisfacen las siguientes relaciones:

$$p_{nn} = q,\ p_{ii} = q^2,\ p_{ii+1} p_{i+1i} = q^{-2},\ 1 \leq i < n;$$

$$p_{ij} p_{ji} = 1,\ j > i+1.$$

El grupo H de los elementos de grupo pueden satisfacer relaciones adicionales arbitrarias que sean compatibles con las reglas conmutativas anteriores.

El coradical de cada álgebra de Hopf, con los generadores expuestos, coincide con el álgebra de grupo $\mathbf{k}[H]$ del grupo H [44]. El primer componente de la filtración del coradical es un espacio lineal expandido por H y todos los productos de la forma $h \cdot w$, donde w es el elemento primitivo torcido, $\Delta(w) = w \otimes 1 + h_w \otimes w, h_w, h \in H$ [69].

Sea $H\langle X \cup X^-\rangle$ el álgebra de Hopf definida conforme a lo anterior con primitivos torcidos libres x_i, x_i^-. Entonces se tienen los morfismos de álgebra de Hopf $\varphi : H\langle X \cup X^-\rangle \to U_q(\mathfrak{so}_{2n+1})$, $\varphi_1 : H\langle X \cup X^-\rangle \to u_q(\mathfrak{so}_{2n+1})$. El ideal $\ker \varphi$, por definición, es generado por los elementos $\mu_{ij} = x_i x_j^- - p_{ji} x_j^- x_i - \delta_i^j(1 - g_i f_i)$ y los polinomios cuánticos de Serre $S_{ij}(x_i, x_j)$, $S_{ij}(x_i^-, x_j^-)$, $1 \leq i, j \leq n$. Todos estos elementos son torcidos primitivos en $H\langle X \cup X^-\rangle$ [34].

El ideal $\ker \varphi_1$ es generado por μ_{ij} y los dos conjuntos $\mathbf{\Lambda}$, $\mathbf{\Lambda}^{-1}$. Aquí, $\mathbf{\Lambda}$ es el mayor biideal de la subálgebra de Hopf $G\langle X\rangle$ generada por las x_i y las g_i que está contenida en el ideal ordinario generado por todos los productos $x_i x_j$. De manera similar, $\mathbf{\Lambda}^{-1}$ es el mayor ideal de la subálgebra de Hopf $F\langle X^-\rangle$ generada por las x_i^- y las f_i que está contenida en el ideal generado por $x_i^- x_j^-$.

Si q no es una raíz de 1, entonces $\mathbf{\Lambda}$ y $\mathbf{\Lambda}^-$ son generados por los polinomios cuánticos de Serre. Así, en este caso $\varphi_1 = \varphi$ y $u_q(\mathfrak{so}_{2n+1}) = U_q(\mathfrak{so}_{2n+1})$ tiene rango combinatorio uno. Por esta razón, en adelante supondremos que q tiene un orden finito multiplicativo $t > 4$. Bajo dicha condición $\varphi_1 \neq \varphi$, puesto que el $\ker \varphi_1$ contiene al menos al elemento primitivo x_n^t que no pertenece al $\ker \varphi$. De hecho los generadores explícitos de los ideales $\mathbf{\Lambda}$, $\mathbf{\Lambda}^-$ tienen la forma $[u]^{h_u}$, donde $[u]$ corre sobre el conjunto de los generadores Poincarè-Birkhoff-Witt (PBW), mientras que $h_u = t$ o $h_u = t/2$ [41].

5.2. Combinatoria de palabras

Para describir y trabajar con los generadores PBW, en esta sección abordaremos las nociones combinatorias básicas expuestas en el Capítulo 3 en el presente contexto. El análisis contemplará en la subálgebra cuántica de Borel positiva, la subálgebra generada por las $g_i^{\pm}$ y x_i. En el conjunto de todas las palabras en las x_i, fijaremos el orden lexicográfico con prioridad de izquierda a derecha considerando $x_1 > x_2 > \ldots > x_n$, donde el comienzo propio de una palabra es considerado como mayor que la palabra misma.

Recordemos que una palabra no vacía u se llama *palabra estándar* si $vw > wv$ para cada descomposición $u = vw$ con v, w no vacías. Una palabra *no asociativa* es aquella en la que el arreglo de corchetes $[,]$ muestra la aplicación de la multiplicación. Si $[u]$ denota una palabra no asociativa, entonces u denota una palabra asociativa obtenida de $[u]$ al remover los corchetes. El conjunto de *palabras no asociativas estándar* es el mayor conjunto SL que contiene todas las variables x_i y satisface las siguientes propiedades:

1. Si $[u] = [[v]\,[w]] \in SL$, entonces $[v]\,, [w] \in SL$, y $v > w$ son estándar.

2. Si $[u] = [[[v_1]\,[v_2]]\,[w]] \in SL$, entonces $v_2 \leq w$.

Cada palabra estándar tiene sólo una alineación de corchetes tal que su forma no asociativa es estándar [63]. Para encontrar dicha alineación, se emplea el siguiente procedimiento inductivo:

5.1 Definición. Una *súper letra* es un polinomio que iguala a una palabra no asociativa en el que los corchetes se encuentran definidos como $[u, v] = uv - p(u, v)vu$, mientras que $p(u, v)$ es el mapeo bimultiplicativo definido en palabras tal que $p(x_i, x_j) = p_{ij}$. Una *súper palabra* es una palabra con súper letras.

Por el teorema de Shirshov, toda palabra estándar u define sólo una súper letra; en adelante, la denotaremos como $[u]$. El orden de las súper letras está definido de forma natural: $[u] > [v] \Leftrightarrow u > v$.

En lo sucesivo, fijaremos un homogéneo en cada x_i bi-ideal I de $G\langle X\rangle$ siempre que $\ker\varphi \cap G\langle X\rangle \subseteq I \subseteq \mathbf{\Lambda}$. En el artículo de Kharchenko y Andrade [42] se muestra que el biideal $\mathbf{\Lambda}$ es homogéneo.

5.2 Definición. Una súper letra $[u]$ se llama *dura en* $G\langle X\rangle / I$ si su valor en $G\langle X\rangle / I$ no es una combinación lineal de valores de súper palabras menores a $[u]$ súper letras.

5.3 Definición. Se dice que la *altura* de una súper letra dura $[u]$ en $G\langle X\rangle / I$ es igual a $h = h([u])$ si h es el menor número tal que: primero, $p(u, v)$ es la s-ésima raíz primitiva de 1, o bien $h = s$ o $h = sl^r$, donde $l = \mathrm{char}(\mathbf{k})$; y además, el valor de $[u]^h$ en $G\langle X\rangle / I$ es una combinación lineal de súper palabras en menos de $[u]$ súper letras. Si no existe tal número, la altura es infinita.

Por [35, Teorema 2], los valores de todas las súper letras duras en $G\langle X\rangle / I$ sobre $\mathbf{k}[G]$; esto es, el conjunto de todos los productos

$$g\,[u_1]^{n_1}\,[u_2]^{n_2}\cdots[u_k]^{n_k}\,, \qquad [u_1] < [u_2] < \cdots < [u_k]\,, \qquad n_i < h\,([u_i])\,, \quad g \in G$$

forman una base de $G\langle X\rangle / I$.

Si $I = \ker\varphi \cap G\langle X\rangle$, esto es, $G\langle X\rangle/I = U_q^+(\mathfrak{so}_{2n+1})$, entonces las súper letras duras son las descritas en [37]. Sea x_i, $n < i \leq 2n$ el generador x_{2n-i+1}. Respectivamente, $u(k,m)$, $1 \leq k \leq m \leq 2n$, es la palabra $x_k x_{k+1} \cdots x_{m-1} x_m$. Si $1 \leq i \leq 2n$, entonces $\psi(i)$ denota el número $2n-i+1$, tal que $x_i = x_{\psi(i)}$. La palabra $u(k,m)$ es estándar si y sólo si $m < \psi(k)$. En el Teorema B_n de la citada referencia, se establece particularmente que $\mathfrak{B} \stackrel{\text{def}}{=} \{[u(k,m)] \,|k \leq m \leq \psi(k)\}$ es el conjunto completo de súper letras duras en $U_q^+(\mathfrak{so}_{2n+1})$, y cada una de ellas tiene una altura infinita.

5.4 Proposición. *El conjunto $\mathfrak{B}$ es el conjunto generadores PBW de $G\langle X\rangle/I$ sobre $\mathbf{k}[G]$. El ideal I está definido de forma única por las alturas de $\mathfrak{B}$. Concretamente, es generado por $[u]^h$, donde $[u] \in \mathfrak{B}$ y h es la altura de $[u]$ en $G\langle X\rangle/I$.*

Demostración. Si $I = \mathbf{\Lambda}$, es decir, $G\langle X\rangle/I = u_q^+(\mathfrak{so}_{2n+1})$, entonces $\mathfrak{B}$ sigue siendo el conjunto de todas las súper letras duras en $u_q^+(\mathfrak{so}_{2n+1})$ [41, Proposición 4.5]. La altura h de $[u(k,m)]$ es igual a t si $m = n$ y t es impar. Si $m \neq n$ y t es par, entonces $h = t/2$. En todos los casos, $[u(k,m)]^h \in \mathbf{\Lambda}$.

La definición de súper letra dura implica que una súper letra dura en $G\langle X\rangle/\mathbf{\Lambda} = u_q^+(\mathfrak{so}_{2n+1})$ es también dura en $G\langle X\rangle/I$, mientras que una dura en $G\langle X\rangle/I$ es dura también en $G\langle X\rangle/\ker\varphi \cap G\langle X\rangle = U_q^+(\mathfrak{so}_{2n+1})$. Así, el mismo conjunto $\mathfrak{B}$ es el conjunto de todas las súper letras duras en $G\langle X\rangle/I$. Además, si h es la altura de $[u(k,m)]$ en $G\langle X\rangle/I$, entonces en $G\langle X\rangle/I$ se tiene que

$$[u(k,m)]^h = \sum_i \alpha_i \prod_j [u(k_{ij}, m_{ij})], \tag{5.1}$$

donde $[u(k_{ij}, m_{ij})]$ son menores a $[u(k,m)]$ súper letras duras.

La lista de las súper letras duras menores es: $[u(k,s)]$, $m < s < \psi(k)$ y $[u(l,r)]$, $k < l \leq r < \psi(l)$. El primer tipo de dichas súper letras depende solamente de x_k, y son lineales en x_k. Puesto que $[u(k,m)]^h$ tiene grado h en x_k, en cada sumando de (5.1) hay h súper letras del tipo $[u(k,s)]$ con $m < s < \psi(k)$. Sin embargo, en este caso el grado del producto $\prod_j [u(k_{ij}, m_{ij})]$ en x_{m+1} es mayor a el de $[u(k,m)]^h$. En efecto, si $m \geq n$, entonces $\deg_{m+1}([u(k,s)]) = 2$, $\deg_{m+1}\left(\prod_j [u(k_{ij}, m_{ij})]\right) \geq 2h$, mientras que $\deg_{m+1}\left([u(k,m)]^h\right) = h$. Si $m < n$, entonces $\deg_{m+1}([u(k,s)]) = 1$, mientras que $\deg_{m+1}\left([u(k,m)]^h\right) = 0$. Por lo tanto, la suma en (5.1) es vacía, y entonces se sigue que $[u(k,m)]^h \in I$.

La alineación de los corchetes en $[u(k,m)]$ se da por medio del algoritmo expuesto y en ocasiones puede complicarse. No obstante, el valor de $[u(k,m)]$ en $U_q^+(\mathfrak{so}_{2n+1})$ es casi independiente de la alineación de éstos. Definimos los arreglos de $u(k,m)$ como sigue:

$$u[k,m] = \begin{cases} [[[\ldots,[x_k,x_{k+1}],\ldots],x_{m+1}],x_m], & \text{si } m < \psi(k); \\ [x_k,[x_{k+1},[\ldots,[x_{m-1},x_m]\ldots]]], & \text{si } m > \psi(k); \\ \beta[u[n+1,m],u[k,n]], & \text{si } m = \psi(k), \end{cases}$$

donde $\beta = -p(u(n+1,m),u(k,n))^{-1}$. Por [41, Proposición 4.1], en $U_q^+(\mathfrak{so}_{2n+1})$ tenemos que $[u(k,m)] = u[k,m]$ siendo $u(k,m)$ una palabra estándar.

□

5.5 Lema. *Si $m \leq n$ o $k > n$, entonces el valor de $u[k,m]$ en $U_q^+(\mathfrak{so}_{2n+1})$ es independiente de la alineación precisa de los corchetes. Si $k \leq n < m$, $m \neq \psi(k)$, entonces*

$$u[k,m] = [u[k,n],u[n+1,m]] \sim [u[n+1,m],u[k,n]]. \tag{5.2}$$

Aquí, $\sim$ denota la igualdad proyectiva: $a \equiv b$ si y sólo si $a = \alpha b$, donde $0 \neq \alpha \in \mathbf{k}$.

Demostración. La primera afirmación se sigue de [41, Lema 2.1], mientras que la segunda de [41, Corolario 3.13]. □

El coproducto de los elementos $u[k,m]$, $k \leq m \leq 2n$ tiene la siguiente forma:

$$\begin{aligned} \Delta(u[k,m]) = {} & u[k,m] \otimes 1 + g_k g_{k+1} \cdots g_m \otimes u[k,m] \\ & + \sum_{i=k}^{m-1} \tau_i \left(1 - q^{-2}\right) g_k g_{k+1} \cdots g_i u[i+1,m] \otimes u[k,i], \end{aligned} \tag{5.3}$$

donde $\tau_s = 1$ para todas las s excepto $\tau_n = q$ (véase [41, Teorema 4.3]). Para el caso en el que $n = 2$, se sugiere revisar [4, (3) y (5)].

La antípoda σ satisface

$$g_k g_{k+1} \cdots g_m \sigma\left(u\left[k,m\right]\right) \sim u\left[\psi\left(m\right),\psi\left(k\right)\right], \tag{5.4}$$

donde como arriba $\psi\left(i\right) = 2n - i + 1$; véase [40, (4.3)].

5.6 Corolario. *Cada elemento w torcido primitivo homogéneo en $G\left\langle X\right\rangle /I$ de grado total mayor a 1 tiene la forma $w = \alpha\left[u\right]^h$, $\alpha \in \mathbf{k}$, donde $[u] \in \mathfrak{B}$, mientras $h = h_u$ o $h = h_u l^s$ en el caso de que la característica sea $l > 0$.*

Demostración. Por [37, Lema 4.9], la descomposición de w en la base PBW tiene la forma $w = \alpha\left[u\right]^h + \sum_i \alpha_i W_i$, donde W_i son súper palabras base en menos de $[u]$ súper letras, y $h = t_u$ o $h = t_u l^s$ o $h = 1$. En la proposición anterior, hemos visto que el multigrado (como vector de grados en x_i) de $\left[u\right]^h$ no es la suma de multigrados de menos de $[u]$ súper letras. Por lo tanto, $w = \alpha\left[u\right]^h$. El coproducto de la fórmula (5.3) muestra que ninguna de las $[u]$, $u \neq x_i$ es primitiva en $G\left\langle X\right\rangle /\mathbf{\Lambda}$. Así, $h \neq 1$.

□

5.7 Lema. *Si $k \leq i < j < \psi(k)$, entonces en $U_q^+(\mathfrak{so}_{2n+1})$ se tiene que*

$$\left[u\left[k,i\right], u\left[k,j\right]\right] = 0$$

a menos que $j = \psi(i) - 1$.

Demostración. La palabra $u\left(k,i\right)u\left(k,j\right)$ es estándar. El algoritmo para alinear los corchetes en palabras estándar muestra que

$$\left[u\left(k,i\right)u\left(k,j\right)\right] = \left[\left[u\left(k,i\right)\right], \left[u\left(k,j\right)\right]\right] = \left[u\left[k,i\right], u\left[k,j\right]\right].$$

Así, sólo falta probar que $\left[u\left(k,i\right)u\left(k,j\right)\right] = 0$ en $U_q^+\left(\mathfrak{so}_{2n+1}\right)$.

La súper letra $\left[u\left(k,i\right)u\left(k,j\right)\right]$ no es dura porque no pertenece a la lista de $\mathfrak{B}$ de súper letras duras. Por tanto, el valor de $\left[u\left(k,i\right)u\left(k,j\right)\right]$ en $U_q^+\left(\mathfrak{so}_{2n+1}\right)$ es una combinación lineal de palabras en súper letras duras que son menores que $\left[u\left(k,i\right)u\left(k,j\right)\right]$. Dichas súper letras duras, son todas $\left[u\left(k,s\right)\right]$, $i < s < \psi\left(k\right)$ y $\left[u\left(l,r\right)\right]$, $k < l \leq r < \psi\left(l\right)$.

Sólo el primer tipo de súper letras depende de x_k y son lineales en x_k. Puesto que $[u(k,i)\,u(k,j)]$ tiene grado 2 en x_k, en la descomposición de $[u(k,i)\,u(k,j)]$, hay dos súper letras del tipo $[u(k,s)]$. Consideremos las siguientes dos opciones:

i) $j \leq n$ o $n \leq i$. En este caso, el grado del producto $[u(k,s_1)] \cdot [u(k,s_2)]$ en x_{i+1} es mayor que aquel de $[u(k,i)\,u(k,j)]$. Por lo tanto, la combinación lineal es vacía, y $[u(k,i)\,u(k,j)] = 0$.

ii) $i < n < j$, $j \neq \psi(i) - 1$. Por el Lema 5.5, tenemos que $[k,j] \sim [u[k,n], u[n+1,j]]$. Al mismo tiempo, $[u[k,i], u[k,n]] = 0$ debido al caso i) con $j \leftarrow n$, mientras que $[u[k,i], u[n+1,j]] = 0$ debido a [41, Proposición 3.15] con $m \leftarrow j$, $j \leftarrow n$. Resta aplicar la identidad aditiva $[u, v \cdot w] = [u,v] \cdot w + p(u,v)\, v \cdot [u,w]$.

□

5.8 Ejemplo. Si $k = n-1$, $i = n-1$, $j = n+1 = \psi(i) - 1$, entonces $[u[k,i], u[k,j]] = [x_{n-1}, [[x_{n-1}, x_n], x_n]] \sim [x_{n-1}, x_n]^2 \neq 0$.

5.3. Constantes del cálculo diferencial

Sea $\mathfrak{U}$ una subálgebra de $U_q^+(\mathfrak{so}_{2n+1})$ generada por x_i. Esta subálgebra tiene un cálculo diferencial con derivadas parciales ∂_i, $1 \leq i \leq n$, que satisface

$$\partial_i(x_j) = \delta_i^j,\ \partial_i(uv) = \partial_i(u) + p(u, x_i)u \cdot \partial_i(v). \tag{5.5}$$

Las derivadas parciales se conectan con el cálculo con el coproducto:

$$\Delta(u) \equiv u \otimes 1 + \sum_i g_i \partial_i(u) \otimes x_i \ (\mathrm{mod}\ G\mathfrak{U} \otimes \mathfrak{U}^{[2]}), \tag{5.6}$$

donde $\mathfrak{U}^{[2]}$ es el ideal de $\mathfrak{U}$ generado por $x_i x_j$, $1 \leq i,j \leq n$. La coasociatividad del coproducto implica

$$\Delta\left(\partial_i(u)\right) = \sum_{(u)} g_i^{-1} u^{(1)} \otimes \partial_i\left(u^{(2)}\right), \tag{5.7}$$

donde se emplea la notación de Sweedler $\Delta(u) = \sum_{(u)} u^{(1)} \otimes u^{(2)}$. Esta igualdad se sigue de [38, Teorema 4.8, (42)], con

$$y_k \leftarrow x_i,\ \frac{\partial^* u}{\partial y_k} \leftarrow g_i \partial_i(u) g_i^{-1},\ \Delta^b(u) = \sum_{(u)} u^{(1)} \mathrm{gr}\left(u^{(2)}\right) - 1 \otimes u^{(2)}.$$

Aquí, $\mathrm{gr}(w) = g_w \in G$ aparece de cada monomial de un elemento homogéneo w bajo las sustituciones $x_i \leftarrow g_i$.

Simétricamente, la ecuación

$$\Delta(u) \equiv \mathrm{gr}(u) \otimes u + \sum_i \mathrm{gr}(u) g_i^{-1} x_i \otimes \partial_i^*(u) \ (\mathrm{mod}\ G\mathfrak{U}^{[2]} \otimes \mathfrak{U}) \tag{5.8}$$

define un cálculo diferencial dual en $\mathfrak{U}$.

Puesto que una antípoda es un morfismo de anticoálgebra (véase [54, Proposición 1.5.10]) estos dos cálculos deberían relacionarse por medio de la antípoda. Sin embargo, si $\mathfrak{U}$ no es σ-invariante: $\sigma(x_i) = -g_i^{-1} x_i \notin \mathfrak{U}$. Por lo tanto, se requiere de la *antípoda trenzada*, σ^b. Por definición, σ^b actúa sobre la palabra u como sigue: $\sigma^b(u) = \mathrm{gr}(u)\sigma(u)$. Por [40, (2.48)], se sabe que la antípoda trenzada satisface

$$\sigma^b\left([u, v]\right) \sim \left[\sigma^b(v), \sigma^b(u)\right]. \tag{5.9}$$

La sustitución $u \leftarrow \sigma^b(u)$ en (5.8) y la propiedad del morfismo de anticoálgebra de σ implica

$$\sigma^b\left(\partial_i^*(u)\right) \sim \partial_i\left(\sigma^b(u)\right). \tag{5.10}$$

Sean $C = \{u \in \mathfrak{U} | \partial_i(u) = 0,\ 1 \leq i \leq n\}$ la subálgebra de constantes del primer cálculo, y $C^* = \{u \in \mathfrak{U} | \partial_i^*(u) = 0,\ 1 \leq i \leq n\}$ la subálgebra de constantes del último. Puesto que el operador ∂_i reduce en uno el grado en x_i de todo monomial y no cambia el grado en otras variables, ambas álgebras, C y C^*, son homogéneos en cada variable. Por medio de la sustitución $u \leftarrow C^*$ en (5.10) tenemos que $\sigma^b(C^*) \subseteq C$. De manera similar, la sustitución $u \leftarrow \left(\sigma^b\right)^{-1}(C)$ implica que $\left(\sigma^b\right)^{-1}(C) \subseteq C^*$; esto es, $C = \sigma^b(C^*)$.

5.9 Teorema. *Sea $C = C^*$ generada como una álgebra por elementos $Tu = [u]^{tu}$ con $[u] = [u(k,m)] \in \mathfrak{B}$, donde $t_u = t$ si $m = n$ o t es impar, y $t_u = t/2$ en otro caso. Todos los elementos T_u son torcidos centrales en $\mathfrak{U}$; esto es, $[f, T_u] = [T_u, f] = 0$ para todas las f homogéneas. En particular, C es el álgebra de polinomios cuánticos: $T_u T_v = q_{uv} T_v T_u$, $q_{uv} q_{vu} = 1$.*

Además, la subálgebra GC generada por G y C es una subálgebra de Hopf, y $U_q^+(\mathfrak{so}_{2n+1})$ es un módulo libre finitamente generado sobre GC de rango t^{n^2} si t es impar, y $t^n(t/2)^{n^2-n}$ si t es par.

Demostración. Primero, se probará que $T_u \in C \cap C^*$. Por [41, Lema 2.10], tenemos que

$$\partial_i\left([u]^{h_u}\right) \sim \underbrace{[[u], [[u], \ldots, [[u]}_{h_u - 1}, \partial_i([u])] \ldots]].$$

Debido a que $[u] = u[k,m]$, $k \leq m < \psi(k)$, la fórmula del coproducto (5.3) con (5.6) implica

$$\partial_i([u]) \sim \begin{cases} u[k+1,m], & \text{si } i = k < m; \\ 0, & \text{si } i \neq k; \\ 1, & \text{si } i = k = m. \end{cases}$$

Al mismo tiempo, [41, Lema 4.4] provee la relación $[[u], [[u], u[k+1,m]]] = 0$ en $U_q^+(\mathfrak{so}_{2n+1})$. Puesto que siempre $h_u > 2$, se tiene que $\partial_i\left([u]^{h_u}\right) = 0$, $1 \leq i \leq n$. De manera similar, [41, Lema 2.10] y (5.9), (5.10) implican

$$\partial_i^* \left([u]^{h_u} \right) \sim [\dots [[\partial_i^* ([u]) \ , \underbrace{[u]], [u]], \dots [u]]}_{h_u - 1}.$$

Por la fórmula del coproducto (5.3) y por la fórmula (5.8), tenemos

$$\partial_i^* (u [k, m]) \sim \begin{cases} u [k, m-1], & \text{si } i \in \{m, \psi (m)\}, m > k; \\ 0, & \text{si } i \notin \{m, \psi (m)\}; \\ 1, & \text{si } i \in \{m, \psi (m)\}, m = k. \end{cases}$$

De manera que el Lema 5.7 conduce a $[u [k, m-1], u [k, m]] = 0$, para $m = \psi (m-1) - 1$, lo que implica que $2m = 2n + 1$. Así, $\partial_i^* \left([u]^{h_u} \right) = 0$, $1 \leq i \leq n$.

Además, la ecuación (5.3) muestra que C es un coideal izquierdo, $\Delta (C) \subseteq G\mathfrak{U} \otimes C$. De hecho, si $c \in C$, entonces

$$0 = \Delta (\partial_i (c)) = \sum_{(c)} g_i^{-1} c^{(1)} \otimes \partial_i \left(c^{(2)} \right).$$

Puesto que las $g_i^{-1} c^{(1)}$ son linealmente independientes, tenemos que $\partial_i \left(c^{(2)} \right) \in C$. Esto implica que $GC^* = G \left(\sigma^b \right)^{-1} (C) = G\sigma^{-1} (C)$ es una álgebra de coideales derechos que contiene el coradical $\mathbf{k} [G]$. Por [39, Teorema 4.1], la subálgebra GC^* tiene una base PBW que puede ser extendida a una base PBW para $U_q^+ (\mathfrak{so}_{2n+1})$. Por otra parte, los generadores PBW pueden elegirse de la siguiente forma: para toda $[u] \in \mathfrak{B}$, elegimos un elemento arbitrario, si lo hay, con la menor m con la forma

$$c_u = [u]^m + \sum_i \alpha_i W_i R_i \in GC^*, \qquad \alpha_i \in \mathbf{k}, \tag{5.11}$$

donde las W_i son súper palabras base no vacías en menos de $[u]$ súper letras, mientras que las R_i son una base de súper palabras en más de, o igual a, $[u]$ súper letras. De acuerdo con [39, Lema 4.3], el número m es igual con 1, o $p (u, u)$ es la r-ésima raíz primitiva de 1 y $m = r$ o (en el caso de una característica positiva) $m = r (\text{char}\mathbf{k})^s$. En

este caso, $p(u,u)$ es una t_u-ésima raíz de 1, y $[u]^{t_u} \in C^*$. Por otro lado, $m \neq 1$. De hecho, de otra manera, por el criterio de Milinski-Schneider (véase [41, Lema 2.11]), tenemos que $c_u - \alpha \in \mathbf{\Lambda}$, $\alpha \in \mathbf{k}$. Sin embargo, esto no es posible, pues (5.11) con $m = 1$ es una combinación lineal de elementos de bases PBW de $u_q^+(\mathfrak{so}_{2n+1})$ con $[u]$ como término líder. Así, podemos elegir $c_u = [u]^{t_u}$. En particular, $C^* = GC^* \cap \mathfrak{U}$, como álgebra, es generada por los elementos $c_u = [u]^{t_u}$ con $[u] \in \mathfrak{B}$. Debido a que todos esos elementos pertenecen a C, se tiene que $C^* \subseteq C$.

El mapeo σ^2 es un automorfismo tal que $\sigma^2(x_i) = p_{ii}x_i$, $\sigma(g_i) = g_i$. Esto implica que $\sigma^2(f) \sim f$ para todo homogéneo en cada polinomio x_i. Por otra parte, $\left(\sigma^b\right)^2(f) = \operatorname{gr}(f)\,\sigma(\operatorname{gr}(f)\,\sigma(f)) = \operatorname{gr}(f)\,f\operatorname{gr}(f)^{-1} \sim f$ también. Aplicando esto a $f = [u]^{t_u}$, se obtiene $\left(\sigma^b\right)^2(C^*) = C^*$. Ahora, aplicaremos σ^b a la relación $C^* \subseteq C = \sigma^b(C^*)$ que ha sido probada. Con ello, se obtiene que

$$C = \sigma^b(C^*) \subseteq \sigma^b(C) = \left(\sigma^b\right)^2(C^*) = C^*.$$

Esto es, $C = C^*$.

Sea $a \in C$. Por (5.5), tenemos que $\partial_i(x_i a) = a$, mientras que $\partial_i(ax_i) = p(a, x_i)\,a$. Por lo tanto,

$$\partial_i([a, x_i]) = p(a, x_i)\,a - p(a, x_i)\,a = 0.$$

Ciertamente, $\partial_k([a, x_i]) = 0$, con $x_k \neq x_i$, por lo que se sigue que $[a, x_i] \in C$ y también $[x_i, a] = \sigma^b([a, x_i]) \in C$. Al mismo tiempo, el grado en x_i de cada generador en T_u es divisible por t o, si t es par, por $t/2$. Por lo tanto, el grado en x_i de cada constante homogénea es divisible por t o $t/2$ si t es par.

Sin embargo, $\deg_i([a, x_i]) = \deg_i([x_i, a]) \equiv 1 \pmod{t/2}$. Esto es posible sólo si $[a, x_i] = [x_i, a] = 0$. Por lo tanto, todas las constantes, particularmente T_u, son torcidas centrales. La altura de $T_u = [u]^{h_u}$ es infinita en GC, puesto que la altura de $[u] \in \mathfrak{B}$ es infinita en $U_q(\mathfrak{so}_{2n+1})$. De manera que C es precisamente el álgebra de polinomios cuánticos en T_u.

Hemos visto que C es un coideal izquierdo; GC^*, un coideal derecho. Puesto que $C^* = C = \sigma^b(C)$, la subálgebra GC es tanto un coideal izquierdo como derecho y es invariante

respecto a la antípoda; esto es, GC es una subálgebra de Hopf.

Finalmente, cada elemento $[u]^r$ tiene una descomposición $[u]^r = [u]^{r_0} \cdot \left([u]^{t_u}\right)^m$, $r_0 < t_u$. Así, los productos

$$\prod_{[u]\in\mathfrak{B}} [u]^{k_u}, \qquad k_u < t_u,$$

forman una base de $U_q^+(\mathfrak{so}_{2n+1})$ sobre GC. El número total de dichos productos es $\prod_{[u]\in\mathfrak{B}} t_u$, es decir, t^{n^2} si t es impar y $t^n\,(t/2)^{n^2-n}$ si t es par. □

5.10 Corolario. *Si $[u] \in \mathfrak{B}$, entonces el ideal I_u de $U_q^+(\mathfrak{so}_{2n+1})$ generado por todos los elementos $[w]^{t_w}$ con $[w] \in \mathfrak{B}$, $w \neq u$ no contiene ninguno de los elementos $[u]^h$, $h \geq 1$.*

Demostración. Supongamos contrariamente que alguna $[u]^h$ pertenece a I_u. Por el Teorema 5.9, los elementos $[w]^{t_w}$ son torcidos centrales. Por lo tanto, los elementos $[w]^{t_w}$, $w \neq u$ generan a I_u como ideal derecho. En particular, en $U_q^+(\mathfrak{so}_{2n+1})$ la siguiente descomposición es válida:

$$[u]^h = \sum_{w\neq u} [w]^{t_w} \cdot V_w. \tag{5.12}$$

Podemos suponer que cada una de las V_w es una combinación lineal de elementos base PBW $[u_1]^{n_1}\,[u_2]^{n_2}\cdots[w]^{n_w}\cdots$. Dado que w^{t_w} es torcido central, tenemos que

$$[w]^{t_w} \cdot [u_1]^{n_1}\,[u_2]^{n_2}\cdots[w]^{n_w}\cdots \sim [u_1]^{n_1}\,[u_2]^{n_2}\cdots[w]^{n_w+t_w\cdots}$$

es nuevamente un elemento base. Por lo tanto, el miembro derecho de (5.12) es una combinación lineal de elementos base, cada uno de los cuales tiene a $[w]$ como factor, con $w \neq u$. Puesto que $[u]^h$ es también un elemento base, (5.12) conduce a una contradicción, por lo que queda demostrado el corolario.

□

5.4. Rango combinatorio de $u_q^+(\mathfrak{so}_{2n+1})$

Consideremos la cadena que define el rango combinatorio:

$$J_0^+ = G\langle X\rangle \cap \ker\varphi \subset J_1^+ \subset J_2^+ \subset \ldots \subset J_k^+ = \mathbf{\Lambda}.$$

5.11 Proposición. *Todas las J_i^+ son ideales de Hopf homogéneos. Sea $[u] = [u(k,m)] \in \mathfrak{B}$.*

Si t es impar o $m \neq n$, entonces $[u]^h \in J_i^+$ si y sólo si $h \geq t_u$ y $m - k < 2^i - 1 + \epsilon_m^n$. Aquí, $\epsilon_m^n = 0$ si $m \geq n$, y $\epsilon_m^n = 1$ en otro caso.

Si t es par y $m = n$, entonces $m-k < 2^{i-1}$ implica $[u]^t \in J_i^+$ mientras que $m-k \geq 2^i-1$ implica $[u]^h \notin J_i^+$.

Demostración. Al hacer inducción sobre i,[37, Teorema B_n, 4] describe todos los elementos primitivos torcidos de $U_q^+(\mathfrak{so}_{2n+1})$. Estos son x_i, $x_i^{t_i}$, $x_i^{t_i l^r}$, $1-g$, $g \in G$ y posiblemente algunas combinaciones lineales de ellos. Recordemos que $t_i = t$ si $i = n$ o t es impar y que $t_i = t/2$ en otro caso. De forma más general, $t_u = t$ si $m = n$ o t es impar, y $t_u = t/2$ en otro caso. Así, J_1^+ es generada por $x_i^{t_i}$. El Corolario 5.10 implica que $[u(k,m)]^h \in J_1^+$ si y sólo si $k = m \leq n$, $h \geq t_i$. Al mismo tiempo, $m - k < 2^1 - 1 + \epsilon_m^n$ y $m < \psi(k)$, equivale a $k = m \leq n$, mientras $n - k < 2^{1-1}$ significa que $k = n$.

Supongamos que la afirmación es válida para J_{i-1}^+. El Corolario 5.6 implica que todo elemento primitivo torcido de $G\langle X\rangle / J_{i-1}^+$ es proporcional a $[u]^h$ con $[u] \in \mathfrak{B}$, $h = t_u$, o $h = t_u l^r$. Puesto que J_{i-1}^+ es un ideal de Hopf homogéneo, por la suposición inductiva, cada componente homogéneo de un elemento primitivo torcido de $G\langle X\rangle / J_{i-1}^+$ es de nuevo primitivo torcido. Así, J_i^+ es generada tanto por J_{i-1}^+ y todos los elementos $[u]^h$ que son primitivos torcidos en $G\langle X\rangle / J_{i-1}^+$. En particular, J_i^+ es un ideal de Hopf homogéneo. Por otra parte, el Corolario 5.10 muestra que $[u]^h \in J_i^+$ si y sólo si $[u]^{h'}$, $h' \leq h$ se encuentra en la lista de los primitivos torcidos de $G\langle X\rangle / J_{i-1}^+$.

Se mostrará primero que si $m - k < 2^i - 1 + \epsilon_m^n$ o (en caso de que $m = n$ y t par) $m-k < 2^{i-1}$, entonces $[u]^{t_u}$ con $u = u(k,m)$ es primitivo torcido en $G\langle X\rangle / J_{i-1}^+$. Por el Teorema 5.9, la subálgebra GC generada sobre G por los elementos $T_u = [u]^{t_u}$, $[u] \in \mathfrak{B}$ es una subálgebra de Hopf. Por lo tanto, existe una descomposición

$$\Delta\left([u]^{t_u}\right) = \sum_{(c)} \mathrm{gr}\left(c^{(2)}\right) c^{(1)} \otimes c^{(2)}, \tag{5.13}$$

tal que $c^{(1)}$, $c^{(2)}$ son palabras (productos) en T_u. Fijemos un tensor $c^{(1)} \otimes c^{(2)}$ distinto de cero en $G\langle X\rangle / J_{i-1}^{+} \otimes G\langle X\rangle / J_{i-1}^{+}$, con $c^{(1)}$ y $c^{(2)}$ no vacíos. Ciertamente, ninguno de los factores en $c^1 = \prod_{\mu\in M_1} [u_\mu]^{t_\mu}$ y $c^2 = \prod_{\mu\in M_2} [u_\mu]^{t_\mu}$ es cero en $G\langle X\rangle / J_{i-1}^{+}$. Así, por el supuesto inductivo, tenemos que $m_\mu - k_\mu \geq 2^{i-1} - 1 + \epsilon_{m_\mu}^n$ o (si $m_\mu = n$ y t es par) $m_\mu - k_\mu \geq 2^{i-2}$, donde $u_\mu = u(k_\mu, m_\mu)$. El grado total del tensor es igual al grado total de $[u]^{t_u}$. Al mismo tiempo, el grado total de $[u]^{t_u}$ es igual a $(m-k+1)\,t_u$. Así, tenemos

$$(m-k+1)\,t_u = \sum_{\mu\in M_1\cup M_2} (m_\mu - k_\mu + 1)\,t_\mu. \tag{5.14}$$

Si t es impar, entonces $t_u = t_\mu = t$, mientras que la ecuación anterior con las condiciones $m-k$ y $m_\mu - k_\mu$ implica

$$2^i + \epsilon_m^n > m - k + 1 \geq \sum_{\mu\in M_1\cup M_2} \left(2^{i-1} + \epsilon_{m_\mu}^n\right). \tag{5.15}$$

Por supuesto, $2^i + 1 < 3\cdot 2^{i-1}$, para $i > 1$. Así, cada uno de los conjuntos M_1, M_2 tiene precisamente un elemento: $M_1 = \{1\}$, $M_2 = \{2\}$. Como resultado, (5.15) implica que $\epsilon_m^n > \epsilon_{m_1}^n + \epsilon_{m_2}^n$. Esto es posible sólo si $\epsilon_m^n = 1$, $\epsilon_{m_1}^n = \epsilon_{m_2}^n = 0$; esto es, si $m > n$, $m_1 \leq n$, y $m_2 \leq n$. Sin embargo, en este caso la diferencia entre el lado izquierdo y el derecho de la ecuación (5.15) es igual a 1. Por esta razón, la última desigualdad de (5.15) es una igualdad, y $m_1 - k_1 = m_2 - k_2 = 2^{i-1} - 1$. Puesto que $2t = \deg_n\left([u_1]^t\right) + \deg_n\left([u_2]^t\right)$, se tiene que $m_1 = m_2 = n$. Esto implica que $k_1 = k_2$, lo cual es una contradicción, pues $\deg_k\left([u_1]^t\right) + \deg_k\left([u_2]^t\right) = 2\deg_k\left([u_1]^t\right)$ es 0 o $2t$, mientras que $\deg_k\left([u]^t\right) = t$.

Si t es par y $m \neq n$, entonces $t_u = t/2$. Si ninguno de los m_μ es igual a n, entonces tenemos de nuevo (5.15), lo cual implica la misma contradicción. Asumamos que una de las m_μ, digamos m_1 (esto es $\mu = 1$), es igual a n. En este caso, $t_{u_1} = t$, mientras que $\deg_n\left([u_1]^t\right) = \deg_n\left([u]^{t/2}\right)$. De tal modo que ninguna de las m_μ con $\mu \neq 1$ depende de x_u; esto es, $m_n < n$. Puesto que $M_1 \cup M_2$ tiene al menos dos elementos diferentes, vemos que (5.14) implica una contradicción:

$$2^i + 1 > m - k + 1 \geq \left(2^{i-2} + 1\right) \cdot 2 + \sum_{\mu \neq 1} 2^{i-1} \geq 2^i + 2. \tag{5.16}$$

Si t es par y $m = n$, entonces $t_u = t$, y tenemos la condición $m - k < 2^{i-1}$. La ecuación (5.14) implica que

$$\left(2^{i-1} + 1\right) t > (m - k + 1)\, t \geq \sum_{m_\mu \neq n} \left(2^{i-1} + \epsilon_{m_\mu}^n\right) \frac{t}{2} + \sum_{m_\mu = n} \left(2^{i-2} + 1\right) t, \tag{5.17}$$

o, equivalentemente, que

$$2^i + 2 < \sum_{m_\mu \neq n} \left(2^{i-1} + \epsilon_{m_\mu}^n\right) + \sum_{m_\mu = n} \left(2^{i-1} + 2\right). \tag{5.18}$$

Esta desigualdad puede ser válida sólo si la última suma es vacía y si la primera tiene justo dos términos, digamos $\mu = 1$ y $\mu = 2$ (recordemos que $M_1 \cup M_2$ tiene al menos dos elementos distintos). Si ambos $\epsilon_{m_1}^n = 0$ y $\epsilon_{m_2}^n = 0$, entonces el tensor $[u_1]^{t/2} \otimes [u_2]^{t/2}$ es independiente de x_n, lo cual es imposible debido a que $\deg_n \left([u]^t\right) = t$. Por lo tanto, $\epsilon_{m_1}^n + \epsilon_{m_2}^n = 1$. En este caso, (5.17) y (5.18) implican

$$2^i + 2 > (m - k + 1) \cdot 2 \geq 2^{i-1} + 2^{i-1} + 1 > 2^i, \tag{5.19}$$

lo cual tampoco es posible debido a que no hay números pares entre 2^i y $2^i + 2$.

Ahora, se mostrará que si $m - k \geq 2^i - 1 + \epsilon_m^n$, entonces $[u]^h$ con $u = u\,(k, m)$ no es primitivo torcido en $G\langle X\rangle / J_{i-1}^+$. Sea s un número arbitrario menor a n. Analizaremos todos los tensores de la descomposición

$$\Delta\left([u]^h\right) = \left(\Delta\left([u]\right)\right)^h = \sum_{(c)} c^{(1)} \otimes c^{(2)}$$

tal que $\deg_s\left(c^{(2)}\right) = h$, $\deg_{s+1}\left(c^{(2)}\right) = 0$. Por la fórmula del coproducto (5.3), cada tensor de dicha descomposición tiene la forma

$$\alpha g a_1 a_2 \cdots a_h \otimes b_1 b_2 \cdots b_h,$$

donde $a_\lambda = u\left[1 + i_\lambda, m\right]$, $b_\lambda = u\left[k, i_\lambda\right]$. Puesto que $\deg_{s+1}\left(b_\lambda\right) = 0$, tenemos que $i_\lambda \leq s$. Por lo tanto, la desigualdad $s < n$ implica que $\deg_s\left(b_\lambda\right) \leq 1$. Al mismo tiempo $\sum_{\lambda=1}^{h} \deg_s\left(b_\lambda\right) = \deg_s\left(c^{(2)}\right) = h$. Esto es, $\deg_s\left(b_\lambda\right) = 1$, para toda λ. En particular, $i_\lambda \geq s$. Por lo tanto, $i_\lambda = s$ para toda λ, y hay un único tensor de los grados requeridos en la descomposición:

$$\alpha g_k^h g_{k+1}^h \cdots g_s^h u\left[s+1, m\right]^h \otimes u\left[k, s\right]^h, \qquad \alpha \neq 0. \tag{5.20}$$

Por la suposición inductiva $u\left[k, s\right]^h \notin J_{i-1}^+$ si $s - k \geq 2^{i-1} - 1$. Al mismo tiempo $u\left[s+1, m\right]$ o $\sigma^b\left(u\left[s+1, m\right]\right) = u\left[\psi\left(m\right), \psi\left(s+1\right)\right]$ pertenece a $\mathfrak{B}$, a menos que $m = \psi\left(s+1\right)$. Por ello, empleando nuevamente el supuesto inductivo, $u\left[s+1, m\right]^h \notin J_{i-1}^+$ dado que $m - s - 1 \geq 2^{i-1} - 1 + \epsilon_m^n$, $m \neq \psi\left(s+1\right)$. Por practicidad, denotaremos $s_{\min} = 2^{i-1} - 1 + k$, $s_{\max} = m - 2^{i-1} - \epsilon_m^n$.

Para mostrar que $[u]^h$ no es primitivo torcido en $G\left\langle X\right\rangle / J_{i-1}^+$, resta encontrar al menos un punto s que satisfaga $s < n$, $m \neq \psi\left(s+1\right)$ en el intervalo $[s_{\min}, s_{\max}]$. Este intervalo es no vacío para $s_{\max} - s_{\min} = m - k - 2^i + 1 - \epsilon_m^n \geq 0$. Si $m \leq n$, entonces ciertamente todos los puntos en el intervalo satisfacen las desigualdades requeridas. Sea $m > n$; esto es, sea $\epsilon_m^n = 1$. En este caso, $s_{\min} + s_{\max} = k + m - 2 \leq 2n - 2$, para $m < \psi\left(s+1\right)$.

Si el intervalo contiene al menos dos puntos, $s_{\min} \leq s_{\max} - 1$, entonces $2s_{\min} \leq s_{\min} + s_{\max} - 1 \leq 2n - 3$. Así, $s_{\min} \leq n - 2$; esto es, el intervalo contiene al menos dos puntos que satisfacen $s < n$. Ciertamente, uno de ellos satisface que $m \neq \psi\left(s+1\right)$.

Si el intervalo contiene un sólo punto, $s = s_{\min} = s_{\max}$, entonces $m + s = m + s_{\max} = 2m - 2^{i-1} - 1$ es un número impar (recordemos que en este caso $\epsilon_m^n = 1$ y, por supuesto, $i > 1$). Al mismo tiempo, $m = \psi\left(s+1\right)$ es equivalente a $m + s = 2n$. Así, $m \neq \psi\left(s+1\right)$.

□

5.12 Teorema. *El rango combinatorio de $u_q^+(\mathfrak{so}_{2n+1})$ es igual a $\lfloor \log_2(n-1) \rfloor + 2$.*

Demostración. Primero, notemos que J_κ^+ con $\kappa = \lfloor \log_2(n-1) \rfloor + 2$ contiene todos los elementos $[u(k,m)]^{t_u}$. Si $m > n$, se tiene que $m - k \leq 2n - 2 = 2^{1+\log_2(n-1)} < 2^{2+\lfloor \log_2(n-1) \rfloor} = 2^\kappa - 1 + \epsilon_m^n$, para $a < 1 + \lfloor a \rfloor$. Por la Proposición 5.11, tenemos que $[u(k,m)]^{t_u} \in J_\kappa^+$.

Si $m < n$, al usar las desigualdades anteriores, tenemos que $m-k \leq n-2 \leq (2n-2)-1 < 2^\kappa - 1$; esto es, sigue siendo cierto que $[u(k,m)]^{t_u} \in J_\kappa^+$.

Si $m = n$ entonces $m - k \leq n - 1 = 2^{\log_2(n-1)} < 2^{1+\lfloor \log_2(n-1) \rfloor} = 2^{\kappa-1} < 2^\kappa - 1$. Nuevamente, la Proposición 5.11 implica que en ambos casos (sea t par o impar), $[u(k,n)]^{t_u} \in J_\kappa^+$.

Notemos que $[u(1,2n-1)]^{t_u} \notin J_{\kappa-1}^+$. Tenemos que $(2n-1) - 1 = 2^{1+\log_2(n-1)} \geq 2^{\kappa-1}$, para $a \geq \lfloor a \rfloor$. Puesto que $\epsilon_{2n+1}^n = 1$, la Proposición 5.11 aplica.

□

La subálgebra GC es un ejemplo de una subálgebra de Hopf, de una álgebra de Hopf primitivamente generada, que no es primitivamente generada. Ciertamente, se trata de una álgebra de Hopf punteada.

5.5. Rango combinatorio de $u_q(\mathfrak{so}_{2n+1})$

Los resultados de la sección anterior son también válidos para la subálgebra cuántica de Borel negativa:

5.13 Teorema. *El rango combinatorio de $u_q(\mathfrak{so}_{2n+1})$ es $\lfloor \log_2(n-1) \rfloor + 2$.*

Demostración. En particular, la cadena que define el rango combinatorio tiene la misma longitud:

$$J_0^- = F\left\langle X^- \right\rangle \cap \ker_\varphi \subset J_1^- \subset J_2^- \subset \cdots \subset J_\kappa^- = \mathbf{\Lambda}^-.$$

Sea J_i un ideal de $H\langle X \cup X^-\rangle$ generado por J_i^+ y por J_i^-. Se probará a continuación que

$$J_0 = \ker_\varphi \subset J_1 \subset J_2 \subset \cdots \subset J_\kappa = \mathbf{\Lambda}$$

es precisamente la cadena que define el rango combinatorio de $u_q(\mathfrak{so}_{2n+1})$. Por [43, Proposición 3.4], se obtiene la siguiente descomposición triangular:

$$H\left\langle X \cup X^-\right\rangle / J_i = F\left\langle X^-\right\rangle / J_i^- \otimes_{\mathbf{k}[F]} \mathbf{k}[H] \otimes_{\mathbf{k}[G]} G\langle X\rangle / J_i^+.$$

La última parte de [37, Lema 6.2], establece que todos los elementos primitivos torcidos de $H\langle X \cup X^-\rangle / J_i$ son combinaciones lineales de los elementos primitivos torcidos de $H\langle X^-\rangle / J_i^-$ y $H\langle X\rangle / J_i^+$. De manera que el subideal de $\mathbf{\Lambda}/J_i$, generado por los primitivos torcidos, coincide con J_{i+1}/J_i y el resultado deseado se sigue. □

Conclusiones

Al implementar mecanismos de codificación y decodificación de información es preciso hacer primero un análisis de la complejidad computacional implícita. Identificar las operaciones o pasos que deben ejecutarse en un algoritmo y el número de veces que deben ser realizados permite determinar el tiempo de ejecución del mismo y también, eventualmente, planear estrategias para su reducción, de manera que su implementación en la práctica resulte viable y eficiente. La eficiencia es un tema importante ya que, si bien el constante desarrollo de hardware ha permitido mejorar la velocidad de cálculo, cada vez las aplicaciones computacionales demandan mayor capacidad de cómputo y mayor velocidad. Actualmente, una computadora promedio es capaz de efectuar 10^8 operaciones en menos de un segundo [11].

La eficiencia se mide mediante el número de operaciones que ejecuta el algoritmo en términos del tamaño de sus datos de entrada. Aunque podría pensarse que el aumento de la velocidad con la que se efectúan los cálculos del algoritmo implica un incremento en el número de datos de entrada en la misma proporción, esto no es así. Por ejemplo, supongamos que un algoritmo realiza n^2 comparaciones para ordenar n números y que se requiere un segundo para ordenar 5 números (25 comparaciones). Si se incrementara la velocidad de cálculo 100 veces, en un segundo se podrían realizar 250 comparaciones, es decir, se podrían ordenar 50 números. Esto significa que el incremento en la velocidad permitiría ordenar tan sólo 10 veces más números en lugar de 100 veces más.

La complejidad computacional, en cuanto a tiempo de ejecución se refiere, cuantifica pues el tiempo que le toma a un algoritmo correr como una función de la longitud de la cadena de entrada. La notación O se utiliza para acotar el peor caso del tiempo de corrida de un algoritmo y describe el comportamiento límite de la función cuando el argumento tiende a un valor, usualmente en términos de funciones más simples del mismo orden de crecimiento. Mediante esta notación es posible clasificar funciones bajo la siguiente jerarquía:

$$O(1) < O(\log n) < O(n) < O\left(n^2\right) < \ldots < O\left(n^k\right) < \ldots < O\left(2^n\right) < O(n!)$$

(tiempos constante, logarítmico, lineal, polinomial, exponencial y factorial, respectivamente). De izquierda a derecha, las funciones sucesivas tienen mayor orden de crecimiento que las previas, es decir, los valores de las últimas funciones se incrementan con mayor rapidez que las primeras. Usualmente, se tiene interés en conocer la complejidad computacional asintótica que involucra al tiempo. Un algoritmo de complejidad $O(\log n)$ es considerado altamente eficiente debido a que permite atacar problemas notablemente grandes en un mínimo de tiempo.

En el contexto de la presente investigación, para usar una álgebra de Frobenius como alfabeto de un código en la práctica es necesario introducir de alguna forma el álgebra a la computadora. Los resultados obtenidos muestran que $\lfloor \log_2 (n-1) \rfloor + 2$ pasos para la representación combinatoria ordinaria son suficientes para ello al emplear el grupo cuántico $u_q(\mathfrak{so})_{2n+1}$ (véase [33]). Este resultado es similar a los hallados para los grupos cuánticos $u_q(\mathfrak{sl}_{n+1})$ y $u_q(\mathfrak{so}_{2n})$ (o equivalentemente para la versión multiparamétrica de los kernels de Frobenius-Lusztig de tipo A_n y D_n, respectivamente): $\lfloor \log_2 (n) \rfloor + 1$ y $\lfloor \log_2 (2n-3) \rfloor + 1$. Los detalles del primer resultado se deben a Kharchenko y Andrade [42], mientras que el segundo se encuentra en proceso de publicación como extensión a este estudio por parte de Díaz y Kharchenko [16]. Esto es:

- $A_n : \lfloor \log_2 (n) \rfloor + 1$,
- $B_n : \lfloor \log_2 (n-1) \rfloor + 2$ y
- $D_n : \lfloor \log_2 (2n-3) \rfloor + 1$.

Como se ha expuesto, desde el punto de vista computacional estos números son muy pequeños, por lo que el uso de estas estructuras algebraicas como alfabeto de un código es factible en la práctica y computacionalmente eficiente. Si bien estos hallazgos no revolucionan la Teoría de Códigos, resultan alentadores. Quedan por estudiar los posibles mecanismos de codificación y decodificación para su implementación y se ponen a consideración para futuras investigaciones.

Existen otros problemas abiertos relacionados, por ejemplo, investigar el rango combinatorio de los kernels de Frobenius-Lusztig donde $\mathfrak{g}$ es una álgebra de Lie simple de tipo C_n $(n > 2)$, E (E_6, E_7, E_8), F (F_4) o G (G_2). Para probar el resultado se empleó la fórmula explícita para el coproducto, la cual no se ha probado para las otras clases aún. Es necesario encontrar una fórmula explícita para el coproducto de las clases restantes y, si es posible, hacer el procedimiento análogo al presentado.

Apéndice A

Cuantificación de $\mathfrak{so}_{2n+1}$

En este apartado se aplicarán los resultados generales del Capítulo 3 a la serie infinita B_n de álgebras de Lie nilpotentes definidas por las relaciones de Serre (3.10) o, de forma equivalente, (3.15). Para ello, primero se hará una revisión sobre el caso A_n. Sea $\mathfrak{g}$ cualquier álgebra de Lie de dicho tipo.

A.1 Lema. *Si la palabra estándar u no posee subpalabras del tipo*

$$x_i^s x_j x_i^m, \quad \text{donde } s+m = 1-\alpha_{ij} \tag{A.1}$$

entonces $[u]$ es dura en $U_P(\mathfrak{g})$ súper letra.

Demostración. Sea R definida por los generadores $x_1, \ldots, x_n$ y las relaciones

$$x_i^s x_j x_i^m = 0, \quad \text{donde } s+m = 1-\alpha_{ij}. \tag{A.2}$$

(A.2) implica (3.15). Por lo tanto, R es una imagen homomórfica de $U_P^b(\mathfrak{g})$. El sistema (A.2) es cerrado bajo composiciones dado que la composición de relaciones monomiales siempre tiene la forma $0 = 0$.

Sea u sin subpalabras del tipo (A.1). Entonces el valor de u en R pertenece a la base de R definida en el Lema del Diamante. Si $[u]$ no es dura, entonces, por la versión homogénea del Lema 3.19, u es una combinación lineal de palabras menores en $U_P^b(\mathfrak{g})$. Por lo tanto, u es una combinación lineal de palabras menores en R también. Esto contradice el hecho de que u pertenece a la base de R definida en el Lema del Diamante. □

Teorema A_n**.** *Supongamos que* $\mathfrak{g}$ *es del tipo* A_n*, y* $p_{ii} \neq -1$*. Denotemos por* B *el conjunto de súper letras dado a continuación:*

$$[u_{km}] \stackrel{\text{def}}{=} [x_k x_{k+1} \dots x_m], \quad 1 \leq k \leq m \leq n. \tag{A.3}$$

Las siguientes afirmaciones son válidas:

i) *Los valores de* $[u_{km}]$ *en* $U_P(\mathfrak{g})$ *forman un conjunto de generadores PBW.*

ii) *Cada una de las súper letras* (A.3) *tiene una altura infinita en* $U_P\langle(\mathfrak{g})\rangle$*.*

iii) *Los valores de todas las súper letras no duras en* $U_P(\mathfrak{g})$ *son iguales con cero.*

iv) *Las siguientes relaciones con* (3.22) *forman un sistema de relaciones de Groebner-Shirshov para* $U_P(\mathfrak{g})$*:*

$$\begin{aligned} &[u_0] \stackrel{\text{def}}{=} [x_k x_m] = 0, && 1 \leq k < m-1 < n; \\ &[u_1] \stackrel{\text{def}}{=} [x_k x_{k+1} \dots x_m x_{k+1}] = 0, && 1 \leq k < m \leq n; \\ &[u_2] \stackrel{\text{def}}{=} [x_k x_{k+1} \dots x_m x_k x_{k+1} \dots x_{m+1}] = 0, && 1 \leq k \leq m < n. \end{aligned} \tag{A.4}$$

v) *Si* $p_{11} \neq 1$*, entonces los generadores* x_i*, las constantes* $1-g$*,* $g \in G$*, y en el caso de que* p_{11} *sea una raíz primitiva* t*-ésima de unidad, los elementos* x_i^t*,* $x_i^{tl^k}$ *forman una base del espacio* $\mathfrak{g}_P = L(U_P(\mathfrak{g}))$ *generado por elementos primitivos torcidos. Aquí,* l *es la característica del campo base.*

vi) *Si* $p_{11} = 1$*, entonces los elementos* (A.3) *y, en el caso en el que* $l > 0$*, sus* l^k*-ésimas potencias, junto con* $1-g$*,* $g \in G$ *forman una base de* $\mathfrak{g}_P$*.*

Por el Corolario 3.8, las relaciones (3.10) con una matriz de Cartan A de tipo A_n admite cuantificación si y sólo si

$$p_{ii} = p_{11}, \quad p_{ii+1}p_{i+1i} = p_{11}^{-1}; \quad p_{ij}p_{ji} = 1, \quad i-j > 1. \tag{A.5}$$

En este caso, las relaciones cuantificadas (3.15) toman la forma:

$$x_i x_{i+1}^2 = p_{p_{ii+1}} (1 + p_{i+1i+1}) x_{i+1} x_i x_{i+1} - p_{ii+1}^2 p_{i+1i+1} x_{i+1}^2 x_i, \tag{A.6}$$

$$x_i^2 x_{i+1} = p_{ii+1} (1 + p_{ii}) x_i x_{i+1} x_i - p_{ii+1}^2 p_{ii} x_{i+1} x_i^2, \tag{A.7}$$

$$x_i x_j = p_{ij} x_j x_i, \quad i-j > 1. \tag{A.8}$$

A.2 Definición. Introduzcamos la congruencia $u \equiv_k v$ en $G\langle X\rangle$. Esta congruencia significa que el valor de $u-v$ en $U_P^b(\mathfrak{g})$ pertenece al subespacio generado por los valores de todas las palabras con las letras iniciales x_i, $i \geq k$.

La congruencia recién expuesta admite la multiplicación por la derecha por medio de polinomios arbitrarios, así como la multiplicación por la izquierda por medio del término independiente de las x_{k-1} (véase (A.8)). Por ejemplo, por (A.6) y (A.7) tenemos que

$$x_i x_{i+1}^2 \equiv_{i+1} 0; \quad x_i x_{i+1} x_i \equiv_{i+1} \alpha x_i^2 x_{i+1}, \quad \alpha \neq 0. \tag{A.9}$$

A.3 Lema. *Si $y = x_i$, $m+1 \neq i > k$ o $y = x_i^2$, $m+1 = i > k$, entonces*

$$u_{km} y \equiv_{k+1} 0. \tag{A.10}$$

Demostración. Sea $y = x_{m+1}^2$, $m+1 > k$. Por (A.9) y (A.8) tenemos que $u_{km}y = u_{km-1}\underline{x_m x_{m+1}^2} \equiv_{m+1} 0$. Si $y = x_i$ y $m+1 \neq i > k$, entonces tenemos $u_{km}y = \alpha u_{ki-1}\underline{x_i x_{i+1} x_i} u_{i+2m} \equiv_{i+1} \beta \underline{u_{ki-1} x_i^2} u_{i+1m} \equiv_{k+1} 0$ por el caso anterior. □

A.4 Lema. *Los corchetes en $[u_{km}]$ son ordenados por la izquierda, $[u_{km}] = [x_k\,[u_{k+1m}]]$.*

Demostración. La afirmación se sigue de forma inmediata de las propiedades *vi*) y *ii*). □

A.5 Lema. *Si una palabra no asociativa $[[u_{km}]\,[u_{rs}]]$ es estándar, entonces $k = m \leq r$; o $r = k+1$, $m \geq s$; o $r = k$, $m < s$.*

Demostración. Por definición, $u_{km} > u_{rs}$ si y sólo si $k < r$; o $k = r$, $m < s$. Si $k = m$, entonces $u_{km} = x_k$ y $m \leq r$. Si $k \neq m$, entonces $[u_{km}] = [x_k\,[u_{k+1m}]]$. Por lo tanto, $u_{k+1m} \leq u_{rs}$, es decir, $k+1 > r$; o $k+1 = r$ y $m \geq s$. El primer caso contradice $k < r$ mientras que el último produce $k = r$. Así, las únicas posibilidades son las indicadas en el lema. □

A.6 Lema. *Si $[w] = [[u_{km}]\,[u_{rs}]]$, $n \geq 1$ es una palabra no asociativa estándar, entonces la constitución de $[w]^h$ no iguala la constitución de ninguna súper palabra en menos de $[w]$ súper letras de B.*

Demostración. Las desigualdades en la última columna de la siguiente tabla son válidas para toda $[u] \in B$ que sea menor que las súper letras que se ubican en la misma fila, donde como se dijo anteriormente $\deg_i(u)$ denota el grado de u en x_i:

$$\begin{array}{rll} [x_k u_{k+1s}] & & \deg_k(u) \leq \deg_{s+1}(u); \\ [x_k u_{rs}], & k \leq r \neq k+1 & \deg_k(u) \leq \deg_{k+1}(u); \\ [u_{km} u_{k+1s}], & m \geq s & \deg_k(u) \leq \deg_{m+1}(u); \\ [u_{km} u_{ks}], & m < s & \deg_k(u) \leq \deg_{m+1}(u). \end{array} \tag{A.11}$$

□

Si todas las súper letras de una súper palabra U satisfacen alguna de las desigualdades, entonces U también lo hace. Ninguna de las súper letras en la primera columna satisface la desigualdad del grado en la misma fila. Finalmente, por el Lema A.5, la primera columna contiene todas las palabras no asociativas estándar del tipo $[[u_{km}][u_{rs}]]$.

A.7 Lema. *Si $p_{11} \neq 1$, entonces los valores de $[u_{km}]^h$, $k < m$, $h \geq 1$ no son primitivos torcidos, en particular son cero.*

Demostración. La subálgebra generada por $x_2, \ldots, x_n$ está definida por la matriz de Cartan de tipo A_{n-1}. Esto nos permite emplear inducción sobre n. Si $n = 1$, entonces el lema es correcto en el sentido de que $[u_{km}]^h = x_1^h \neq 0$.

Sea $n > 1$. Si $k > 1$, entonces podemos usar la suposición inductiva directamente. Consideremos la descomposición $\Delta([u_1 m]) = \sum u^{(1)} \otimes u^{(2)}$. Puesto que

$$[u_{1m}] = x_1 [u_{2m}] - p(x_1, u_{2m}) [u_{2m}] x_1, \tag{A.12}$$

$$\Delta([u_{1m}]) = (x_1 \otimes 1 + g_1 \otimes x_1) \Delta([u_{2m}]) \tag{A.13}$$

$$- p(x_1, u_{2m}) \Delta([u_{2m}]) (x_1 \otimes 1 + g_1 \otimes x_1). \tag{A.14}$$

Por lo tanto, la suma de todos los tensores $u^{(1)} \otimes u^{(2)}$ con $\deg_1\left(u^{(2)}\right) = 1$, $\deg_k\left(u^{(2)}\right) = 0$, $k > 1$ tiene la forma $\epsilon g_1 [u_{2m}] \otimes x_1$, donde $\epsilon = 1 - p(x_1, u_{2m}) p(u_{2m}, x_1)$ puesto que $[u_{2m}] g_1 = p(u_{2m}, x_1) g_1 [u_{2m}]$. Por (A.5) tenemos que $p_{ij} p_{ji} = 1$ para $i - 1 > j$. Por lo tanto, $\epsilon = 1 - p_{12} p_{21} = 1 - p_{11}^{-1} \neq 0$.

Esto implica que en la descomposición $\Delta\left([u_{1m}]^h\right) = \sum v^{(1)} \otimes v^{(2)}$ la suma de todos los tensores $v^{(1)} \otimes v^{(2)}$ con $\deg_1\left(v^{(2)}\right) = h$, $\deg_k\left(v^{(2)}\right) = 0$, $k > 1$ es igual con $\epsilon^h [u_{2m}]^h \otimes x_1^h$. Así, $[u_{1m}]^h$ no es primitivo torcido en $U_P(\mathfrak{g})$. □

Con estos elementos, ahora pasamos a la prueba del Teorema A_n, mismo que resulta fundamental para estudiar el caso B_n.

Demostración del Teorema A_n. Mostraremos primero que B satisface las condiciones del Lema 3.20. Por el Lema 3.19, $[w] = [[u_{km}]\,[u_{rs}]]$ es no dura si el valor de $u_{km}u_{rs}$ es una combinación lineal de palabras menores. Para $k = m$, $r = k+1$ tenemos $[w] = [u_{ks}] \in B$. Si $k = m$, $r > k+1$ entonces la palabra $x_k u_{rs}$ puede disminuirse por (A.7) o (A.8). Si $k \neq m$, entonces por el Lema A.5 la palabra $u_{km}u_{rs}$ tiene una subpalabra del tipo u_1 o u_2. De manera que resta probar que los valores en $U_P(\mathfrak{g})$ de u_1 y u_2 son combinaciones lineales de palabras menores.

La palabra u_1 tiene tal representación por el Lema A.3. Consideremos la palabra u_2. Mostraremos por inducción hacia atrás sobre k que

$$u_{km}u_{km+1} \equiv_{k+1} \gamma u_{km+1}u_{km}, \quad \gamma \neq 0. \tag{A.15}$$

Si $k = m$, entonces puede emplearse (A.7) con $i = k$. Sea $k < m$. Transpongamos la segunda letra x_k de u_2 tan a la izquierda como sea posible por (A.8). Obtenemos

$$u_2 = \alpha \underline{x_k x_{k+1} x_k} x_{k+2} \dots x_m x_{k+1} \dots x_{m+1}, \quad \alpha \neq 0.$$

Por (A.7) tenemos

$$u_2 \equiv_{k+1} \beta x_k^2 \left(x_{k+1} x_{k+2} \dots x_m x_{k+1} \dots x_{m+1}\right), \quad \beta \neq 0.$$

Apliquemos la hipótesis inductiva a la palabra en los paréntesis. Dado que x_i, $i > k+1$, conmuta con x_k^2 de acuerdo con la fórmula (A.8) se sigue que

$$u_2 \equiv_{k+1} \gamma \underline{x_k^2 x_{k+1}} x_{k+2} \dots x_{m+1} x_{k+1} \dots x_m.$$

Ahora, queda reemplazar la subpalabra subrayada de acuerdo con (A.7) y luego transponer la segunda letra x_k a su posición inicial por medio de (A.8).

Es importante notar que para reducir u_1 y u_2 no es posible emplear la relación $[x_{n-1}x_n^2] = 0$, ya que $\deg_n(u_1) \leq 1$, $\deg_n(u_2) \leq 1$.

Así, B satisface las condiciones del Lema 3.20. Puesto que ninguna de las $[u_{km}]$ cuenta con subpalabras de la forma (A.1), los lemas A.1 y 3.20 muestran que la primera afirmación es correcta.

Si $[u_{km}]$ tiene altura finita h, entonces el valor del polinomio $[u_{km}]^h$ en $U_P(\mathfrak{g})$ es una combinación lineal de palabras en súper letras duras que son menores a $[u_{km}]$. Sin embargo, por el Lema A.6, esta combinación es trivial, $[u_{km}]^h = 0$, dado que las relaciones definitorias son homogéneas. Por el Lema A.7, la segunda afirmación es correcta para $p_{11} \neq 1$.

De manera similar, consideremos los elementos primitivos torcidos. Puesto que ambas relaciones definitorias y el coproducto son homogéneos, todos los componentes homogéneos del elemento primitivo torcido son primitivos torcidos. Por lo tanto, queda describir todos los elementos primitivos torcidos homogéneos en cada x_i. Sea T tal elemento. Por el Lema 3.21 tenemos que

$$T = [u]^h + \sum \alpha_i W_i,$$

donde $[u]$ es una súper letra dura, $u = u_{km}$ y W_i son súper palabras en menos que $[u]$ súper letras de B. Por la homogeneidad, todas las W_i tienen la misma constitución que $[u_{km}]^h$. Esto significa que el único caso posible es $T = [u_{km}]^h$. Así, por el Lema A.7, la quinta afirmación es también válida.

Si $p_{11} = 1$, entonces $p_{ij}p_{ji} = p_{ii} = 1$ para todas i, j. Estamos pues en las condiciones del Ejemplo 3.5, esto es, $U_P(\mathfrak{g})$ es el álgebra universal envolvente del álgebra de Lie coloreada, $\mathfrak{g}^{\mathrm{col}}$. Además, $[u_{km}] \in \mathfrak{g}^{\mathrm{col}}$ y $[u_{km}]$ son linealmente independientes en $\mathfrak{g}^{\mathrm{col}}$ debido a que son súper letras duras y ninguna de ellas puede ser combinación lineal de palabras menores. Completemos B a una base homogénea B' de $\mathfrak{g}^{\mathrm{col}}$. Entonces, por el teorema PBW para álgebras de Lie coloreadas, los coproductos $b_1^{n_1} \ldots b_k^{n_k}$, $b_1 < \ldots < b_k$ forman una base de $U\left(\mathfrak{g}^{\mathrm{col}}\right) = U_P^b(\mathfrak{g})$. Sin embargo, las palabras monótonas restringidas en B forman también una base de $U_P^b(\mathfrak{g})$. Así, $B' = B$ y todas las súper letras duras tienen altura infinita.

En particular, tenemos que la segunda afirmación es válida en una medida completa. Por otra parte, si $p_{11} = 1$, entonces $p(u_{km}, u_{km}) = 1$ y en consecuencia, para $l = 0$, todos los elementos torcidos primitivos homogéneos se agotan por $[u_{km}]$, en tanto que, para $l > 0$, las potencias $[u_{km}]^{lk}$ les son añadidas ($l \neq 2$ ya que $-1 \neq p_{ii} = 1$).

Hemos probado todos los enunciados, excepto *iii*) y *iv*). Éstos se siguen del Teorema 3.24 y el Lema 3.25 si se demuestra que todas las súper letras no duras $[[u_{km}][u_{rs}]]$ son iguales con cero en $U_P(\mathfrak{g})$. Por la definición homogénea, $[[u_{km}][u_{rs}]]$ es una combinación lineal de súper palabras en menos súper letras duras. Sin embargo, por el Lema A.6, no existen tales súper palabras de la misma constitución. Por lo tanto, por la homogeneidad, la combinación lineal anterior es igual con cero. □

Ahora, procederemos a hacer el análisis análogo para el caso B_n:

Teorema B_n**.** *Sea* $\mathfrak{g}$ *del tipo* B_n*, y* $p_{ii} \neq -1$*,* $1 \leq i < n$*,* $p_{nn}^{[3]} \stackrel{\text{def}}{=} p_{nn}^2 + p_{nn} + 1 \neq 0$*. Denotemos con* B *al conjunto de súper letras dadas a continuación:*

$$\begin{aligned} [u_{km}] &\stackrel{\text{def}}{=} [x_k x_{k+1} \dots x_m], \quad 1 \leq k \leq m \leq n; \\ [w_{km}] &\stackrel{\text{def}}{=} [x_k x_{k+1} \dots x_n \cdot x_n x_{n-1} \dots x_m], \quad 1 \leq k \leq m \leq n. \end{aligned} \tag{A.16}$$

Las siguientes afirmaciones son válidas:

i) *Los valores de* (3.3) *en* $U_P(\mathfrak{g})$ *forman el conjunto de generadores PBW.*

ii) *Toda súper letra* $[u] \in B$ *tiene altura infinita en* $U_P(\mathfrak{g})$*.*

iii) *Las relaciones* (3.22) *con las siguientes forman un sistema de Groebner-Shirshov para* $U_P(\mathfrak{g})$*:*

$$\begin{aligned} [u_0] &\stackrel{\text{def}}{=} [x_k x_m] = 0, && 1 \leq k < m-1 < n; \\ [u_1] &\stackrel{\text{def}}{=} [u_{km} x_{k+1}] = 0, && 1 \leq k < m \leq n, k \neq n-1; \\ [u_2] &\stackrel{\text{def}}{=} [u_{km} u_{km+1}] = 0, && 1 \leq k \leq m < n; \\ [u_3] &\stackrel{\text{def}}{=} [w_{km} x_{k+1}] = 0, && 1 \leq k < m \leq n, k \neq m-2; \\ [u_4] &\stackrel{\text{def}}{=} [w_{kk+1} x_{k+2}] = 0, && 1 \leq k < n-1; \\ [u_5] &\stackrel{\text{def}}{=} [w_{km} w_{km-1}] = 0, && 1 \leq k < m-1 \leq n-1; \\ [u_6] &\stackrel{\text{def}}{=} \left[u_{kn}^2 x_n\right] = 0, && 1 \leq k < n;. \end{aligned} \tag{A.17}$$

iv) *Si* $p_{11} \neq 1$*, entonces los generadores* x_i *y sus potencias* x_i^t*,* $x_i^{tl^k}$*, tales que* p_{ii} *es una raíz primitiva* t*-ésima de 1, junto con las constantes* $1 - g$*,* $g \in G$ *forman una base de* $\mathfrak{g}_P = L(U_P(\mathfrak{g}))$*. Donde* l *es la característica del campo base.*

v) *Si* $p_{nn} = p_{11} = 1$*, entonces se tienen los elementos* (A.16) *y, para* $l > 0$*, sus* l^k*-ésimas potencias, junto con* $1 - g$*,* $g \in G$*, forman una base de* $\mathfrak{g}_P$*. Si* $p_{nn} = -p_{11} = -1$*, entonces* $[u_{kn}]^2$*,* $[u_{kn}]^{2l^k}$ *les son añadidas.*

Recordemos que en el caso B_n, el álgebra $U_P^b(\mathfrak{g})$ está definida por (A.6), (A.7) y (A.8) donde en (A.6) la última relación, $i = n-1$, es reemplazada con

$$x_{n-1} x_n^3 = p_{n-1n} p_{nn}^{[3]} x_n x_{n-1} x_n x_{n-1} x_n^2 - p_{n-1n}^2 p_{nn} p_{nn}^{[3]} x_n^2 x_{n-1} x_n + p_{n-1n}^3 p_{nn}^3 x_n^3 x_{n-1}. \tag{A.18}$$

Por el Corolario 3.8 obtenemos las condiciones de existencia

$$p_{ii} = p_{11}, \quad p_{ii+1}p_{i+1i} = p_{11}^{-1} = p_{nn}^{-2}, \quad 1 \leq i \leq n-1; \quad p_{ij}p_{ji} = 1, \quad i-j > 1. \tag{A.19}$$

Las relaciones (A.6) y (A.18) muestran que

$$x_i x_{i+1}^2 \equiv_{i+1} 0, \quad i < n-1; \quad x_{n-1}x_n^3 \equiv_n 0, \tag{A.20}$$

mientras que las relaciones (A.7) implican que

$$x_i x_{i+1} x_i \equiv_{i+1} \alpha x_i^2 x_{i+1}, \quad \alpha \neq 0. \tag{A.21}$$

Por medio de dichas relaciones y (A.8), (A.18) tenemos que

$$x_{n-2}x_{n-1}\underline{x_n^2 x_{n-1}x_n} \equiv_{n-1} 0. \tag{A.22}$$

A.8 Lema. *Los corchetes en* $[w_{km}]$ *están dados por las fórmulas de recurrencia*

$$\begin{aligned} [w_{km}] &= [x_k\,[w_{k+1m}]\,], \quad \text{si } 1 \leq k < m-1 < n; \\ [w_{kk+1}] &= [[w_{kk+2}]\,x_{k+1}\,], \quad \text{si } 1 \leq k < m-1 < n. \end{aligned} \tag{A.23}$$

Aquí, por definición, $w_{kn+1} = u_{kn}$.

Demostración. Es suficiente con emplear las propiedades *vi*) y luego *i*) y *ii*). □

A.9 Lema. *La palabra no asociativa* $[[w_{km}]\,[w_{rs}]]$ *es estándar sólo en los siguientes casos: i)* $s \geq m > k+1 = r$*; ii)* $s < m, r = k$.

Demostración. Si $[[w_{km}]\,[w_{rs}]]$ es estándar, entonces $w_{km} > w_{rs}$ y, por (A.24), $w_{k+1} \leq w_{rs}$, o $m = k+1$ y $x_{k+1} \leq w_{rs}$. La desigualdad $w_{km} > w_{rs}$ es válida sólo en dos casos: $k < r$ o $k = r$, $m > s$. Se tienen entonces cuatro posibilidades:

i) $k < r$, $k < m-1$, $w_{k+1m} \leq w_{rs}$;

ii) $k < r$, $m = k+1$, $x_{k+1} \leq w_{rs}$;

iii) $k = r$, $m > s$, $k < m-1$, $w_{k+1m}w_{rs}$;

iv) $k = r$, $m > s$, $m = k+1$, $x_{k+1} \leq w_{rs}$.

Sólo la primera y la tercera desigualdad son consistentes, ya que en el segundo caso $x_{k+1} \leq w_{rs}$ implica que $k+1 > r$, mientras que en el cuarto caso $r < s$ y $k = r < s < m = k+1$. Si ahora decodificamos $w_{k+1m} \leq w_{rs}$ en el primer y en el tercer caso, obtenemos las dos posibilidades que se indican en el lema. □

A.10 Lema. *La palabra no asociativa* $[[u_{km}]\,[w_{rs}]]$ *es estándar sólo en los siguientes casos: i)* $k = r$*; y ii)* $k = m < r$*.*

Demostración. La desigualdad $u_{km} > w_{rs}$ significa que $k \leq r$. Puesto que $[u_{km}] = [x_k\,[u_{k+1m}]]$, para $k \neq m$ tenemos que $u_{k+1m} \leq w_{rs}$, y entonces $k+1 > r$ y $k = r$. Si $k = m \neq r$, entonces $x_m > w_{rs}$ y $m < r$. □

A.11 Lema. *La palabra no asociativa* $[[w_{km}]\,[u_{rs}]]$ *es estándar sólo en los siguientes dos casos: i)* $r = k+1 < m$ *y ii)* $r = k+1 = m = s$*.*

Demostración. La desigualdad $w_{km} > u_{rs}$ implica que $r > k$. Si $k < m-1$, entonces por la primera fórmula de (A.24) tenemos que $w_{k+1} \leq u_{rs}$, que es equivalente a $k+1 \geq r$. Por lo tanto, $r = k+1 < m$. Si $k = m-1$, entonces por la segunda fórmula de (A.24) tenemos que $x_{k+1} \leq u_{rs}$, esto es, $k+1 > r$ o $k+1 = r = s$. El primer caso contradice $r > k$, en tanto que el segundo es mencionado en el lema. □

A.12 Lema. *Si* $[u], [v] \in B$*, entonces uno de los enunciados siguientes es correcto:*

i) $[[u]\,[v]]$ *no es una palabra no asociativa estándar;*

ii) uv *contiene una subpalabra de uno de los tipos* $u_0, u_1, u_2, u_3, u_4, u_5, u_6$*;*

iii) $[[u]\,[v]] \in B$*.*

Demostración. La prueba se sigue de los lemas A.5, A.9, A.10 y A.11. □

A.13 Lema. *Si una súper palabra* W *es igual a una de las súper letras* $[u_1] - [u_6]$ *o* $[u_{km}]^h$, $[w_{km}]^h$, $h \geq 1$*, entonces su constitución no es igual a la constitución de ninguna súper palabra en menos que* W *súper letras de* B*.*

Demostración. La prueba es similar a la del Lema A.6 conforme a la siguiente tabla:

$$\begin{array}{ll} [u_{km}], [u_{km}x_{k+1}], [u_{km}u_{km+1}] & \deg_k(u) \leq \deg_{m+1}(u); \\ [w_{km}], [w_{km}x_{k+1}], [w_{km}w_{km+1}] & 2\deg_k(u) \leq \deg_{m-1}(u); \\ [w_{kk+1}x_{k+2}] & \deg_k(u) = 0; \\ \left[u_{kn}^2 x_n\right] & \deg_k(u) \leq \deg_n(u). \end{array} \tag{A.24}$$

□

A.14 Lema. *Si* $y = x_i$, $m-1 \neq i > k$ *o* $y = x_i^2$, $m-1 = i > k$, *entonces*

$$w_{km} y \equiv_{k+1} 0. \tag{A.25}$$

Demostración. Si $i < m-1$, entonces por medio de (A.8) es posible permutar y a la izquierda de x_n^2 y usar el Lema A.3 con $m' = n-1$. Si $y = x_i^2$, $m-1 = i > k$, entonces por el caso anterior, $i < m-1$, tenemos

$$w_{km} y = w_{km+1} \underline{x_m x_{m-1}^2} = \underline{w_{km+1} x_{m-1}} \left(\alpha x_m x_{m-1} + \beta x_{m-1} x_m\right) \equiv_{k+1} 0, \tag{A.26}$$

donde para $m = n$ por definición $w_{kn+1} = u_{kn}$, y $u_{kn} x_{n-1} \equiv_{n-1} 0$.

Si $y = x_i$, $i = m > k$, entonces como $m = n$ podemos usar la segunda igualdad (A.20). Para $m < n$ tenemos $w_{km+1} y = w_{km+1} y_1$ donde $y_1 = x_m^2$. Por lo tanto, por $k < n-1$ podemos emplear (A.26) con $m+1$ en lugar de m. Para $k = n-1$ tenemos que $w_{km} x_n = x_{n-1} x_n^3 \equiv_n 0$.

Finalmente, si $y = x_i$, $i > m > k$, entonces por (A.8) tenemos $w_{km} y = \alpha w_{ki+1} \underline{x_i x_{i-1} x_i} \cdot v$. Para $i = n$ es posible usar (A.22), mientras que para $i < n$, cambiando la palabra subrayada de acuerdo con (A.6), podemos usar los casos considerados anteriormente: $m' - 1 = i'$, donde $m' = i+1$, $i'^{=i}$; y $i' < m' - 1$, donde $m' = i+1$, $i' = i-1$. □

Otra relación interesante aparece si se multiplica (A.18) por x_{n-1} por la izquierda y se sustrae (A.7) con $i = n-1$ multiplicado por la derecha por x_n^2:

$$x_{n-1} x_n x_{n-1} x_n^2 \equiv_n \alpha x_{n-1} x_n^2 x_{n-1} x_n, \tag{A.27}$$

en cuyo caso $\alpha = p_{n-1n} p_{nn}^{[3]} \neq 0$.

A.15 Lema. *Para* $k < s < m \leq n$ *la siguiente relación es válida.*

$$w_{km} w_{ks} \equiv_{k+1} \epsilon w_{ks} w_{km}, \quad \epsilon \neq 0. \tag{A.28}$$

Demostración. Apliquemos inducción hacia atrás sobre k. Para ello, primero transpondremos la segunda letra x_k de $w_{km} w_{ks}$ tan lejos como sea posible por medio de (A.8), y luego cambiaremos el comienzo $x_k x_{k+1} x_k$ de acuerdo con (A.21). Obtenemos entonces

$$w_{km} w_{ks} \equiv_{k+1} \alpha x_k^2 \left(w_{k+1m} w_{k+1s}\right), \quad \alpha \neq 0. \tag{A.29}$$

Para $k+1 < s$ aplicaremos la suposición inductiva a la palabra en el paréntesis y luego, por (A.21) y (A.8), transpondremos x_k a la posición anterior.

El caso en que $k+1 = s = n-1$, la base de la inducción sobre k, se prueba por inducción hacia a atrás sobre s.

Sea $k+1 = s = n-1$. Entonces, $m = n$. Primero, mostraremos que

$$\underline{x_{n-1}x_n^2x_{n-1}x_n}x_nx_{n-1} \equiv_n \alpha x_{n-1}x_n^2x_{n-1}^2x_n^2 + \beta x_{n-1}x_nx_{n-1}^2x_n 3, \quad \alpha \neq 0. \tag{A.30}$$

Por ello, del lado izquierdo transponemos la primera letra x_n gracias a (A.27) a la penúltima posición, y luego reemplazamos el final $x_n^3x_{n-1}$ por (A.18). Se obtiene pues una combinación lineal de tres palabras. Una de ellas iguala a la segunda palabra de (A.30), mientras que las otras dos tienen las formas siguientes,

$$x_{n-1}x_n\underline{x_{n-1}x_nx_{n-1}}x_n^2, \quad \underline{x_{n-1}x_nx_{n-1}x_n^2}x_{n-1}x_n.$$

La primera palabra, por (A.7) se transforma en la forma (A.30). La segunda palabra, luego de aplicársele (A.27) y de reemplazar a $x_{n-1}x_nx_{n-1}$ por (A.7), traerá el término adicional $\underline{x_{n-1}x_n^3}x_{n-1}^2x_n$, al cual es posible aplicar (A.20). El cálculo directo de coeficientes muestra que $\alpha = p_{n-1n}p_{nn\neq 0}$.

Ahora, multiplicaremos (A.30) por x_{n-2}^2 por la izquierda y usaremos (A.7) con $i = n-2$. Obtenemos que $w_{n-2n}w_{n-2n-1}$ con respecto de $\equiv_{n-1}$ es igual con

$$\gamma x_{n-2}x_{n-1}x_n^2\underline{x_{n-2}x_{n-1}^2}x_n^2 + \delta x_{n-2}x_{n-1}x_n\underline{x_{n-2}x_{n-1}^2}x_n^3, \quad \gamma \neq 0. \tag{A.31}$$

Apliquemos (A.20) y luego (A.21) y (A.20) a la segunda palabra. Tenemos que la palabra resultante es igual con cero respecto de $\equiv_{n-1}$. La primera palabra luego de aplicar (A.7) toma la forma

$$\epsilon w_{n-2n-1}w_{n-2n} + \epsilon'\underline{w_{n-2n}x_{n-1}^2}x_{n-2}x_n^2, \quad \epsilon \neq 0.$$

Así, por el Lema A.14, la base de la inducción sobre s queda probada.

Ahora, llevemos a cabo el paso inductivo. Sea $k+1 = s < n-1$. Si $m > s+1 = k+2$, entonces por la hipótesis inductiva sobre s podemos escribir

$$w_{km}w_{ks} = (w_{km}w_{kk+2}x_{k+1}) \equiv_{k+1} \alpha w_{kk+2}w_{km}x_{k+1} = \beta w_{kk+2}\underline{x_kx_{k+1}x_{k+2}x_{k+1}}w_{k+3m}. \tag{A.32}$$

Tomando en consideración (A.25), podemos omitir las palabras que comienzan con x_{k+1}^2, x_{k+2} en tanto transformamos la parte subrayada:

$$x_k \underline{x_{k+1}x_{k+2}x_{k+1}} \equiv \gamma \underline{x_k x_{k+1}^2} x_{k+2} \equiv \delta x_{k+1}x_k x_{k+1}x_{k+2}. \tag{A.33}$$

De este modo, (A.32) queda transformada en (A.28).

Si $m = s+1 = k+2 < n$, entonces la relación (A.29) toma la forma

$$w_{km}w_{ks} \equiv_{k+1} \alpha\epsilon^{-1}x_k^2 w_{k+1k+3}w_{k+1k+3}\underline{x_{k+2}^2 x_{k+1}},$$

o, luego de una sustitución sencilla,

$$w_{km}w_{ks} \equiv_{k+1} \gamma x_k^2 w_{k+1k+3}w_{k+1k+2}\cdot x_{k+1}x_{k+2} + \delta x_k^2 w_{k+1k+3}^2 x_{k+1}x_{k+2}^2.$$

En ambos términos podemos transponer una letra x_k a su posición inicial por medio de (A.21) y (A.8). Tenemos entonces que

$$w_{km}w_{ks} \equiv_{k+1} \gamma' \underline{w_{kk+3}w_{kk+1}} x_{k+2} + \delta' w_{kk+3}^2 x_{k+1}x_{k+2}^2. \tag{A.34}$$

Es posible aplicar (A.28) con $m' = k+3$, $s' = k+1$ al primer término dado que el caso $m > s+1$ está considerado. Por lo tanto, es suficiente con mostrar que el segundo término es igual con cero con respecto de $\equiv_{k+1}$. Cuando transponemos la tercera letra x_{k+1} tan lejos como es posible se obtiene la palabra

$$w_{kk+3}\underline{x_k x_{k+1}x_{k+2}x_{k+1}} w_{k+3k+3}x_{k+2}^2. \tag{A.35}$$

Tomando en consideración (A.25) podemos omitir las palabras que comienzan con x_{k+1} y al transformar la parte subrayada:

$$x_k \underline{x_{k+1}x_{k+2}x_{k+1}} \equiv x_{k+2}\underline{x_k x_{k+1}^2} \equiv x_{k+2}x_{k+1}x_k x_{k+1}. \tag{A.36}$$

Por lo tanto, la palabra (A.35) es igual con $w_{kk+1}\underline{w_{kk+3}x_{k+2}^2}$ con respecto de $\equiv_{k+1}$ y resta sólo aplicar el Lema A.14 dos veces. □

A.16 Lema. *El conjunto B satisface las condiciones del Lema 3.20.*

Demostración. Por los lemas A.12 y 3.19 basta con mostrar que en $U_P^b(\mathfrak{g})$ todas las palabras de la forma $u_0, \ldots, u_6$ son combinaciones lineales de palabras menores. Las palabras u_0 se reducen gracias a (A.8). Las palabras u_1, u_2 se han presentado de esta forma, sin emplear $[x_{n-1}x_n^2] = 0$, en la prueba del teorema anterior. La relación (A.25)

muestra que $u_3 \equiv_{k+1} 0$, $u_4 \equiv_{k+1} 0$. Haciendo $s = m-1$, el Lema A.15 conduce a la representación necesaria para u_5.

Probaremos por inducción hacia atrás sobre k que

$$u_6 \stackrel{\text{def}}{=} u_{kn}^2 x_n \equiv_{k+1} \epsilon u_{kn} x_n u_{kn}, \quad \epsilon \neq 0.$$

Para $k = n-1$ esta igualdad toma la forma (A.27). Sea $k < n-1$. Transpongamos ahora la segunda letra x_k de $u_{kn}^2 x_n$ tan lejos como sea posible por medio de (A.8) y luego apliquemos (A.6). Tenemos pues que

$$u_{kn}^2 x_n \equiv_{k+1} \alpha x_k^2 \left(u_{k+1}^2 x_n\right), \quad \alpha \neq 0.$$

Podemos aplicar la hipótesis inductiva al término del paréntesis y luego, por (A.6) y (A.8), transponer una de las x_k a su posición inicial. □

A.17 Lema. *Si $p_{11} \neq 1$, entonces los valores de los polinomios $[v]^h$, donde $[v] \in B$, $v \neq x_i$, $h \geq 1$ no son primitivos torcidos, en particular, son distintos de cero.*

Demostración. Notemos que para $n > 2$ la subálgebra generada por $x_2, \ldots, x_n$ está definida por la matriz de Cartan de tipo B_{n-1}. Esto nos permite llevar a cabo inducción sobre n con el supuesto adicional de que las afirmaciones $i)$ y $ii)$ del Teorema B_n son válidas para valores menores de n. Es conveniente considerar formalmente las subálgebras generadas $\langle x_i \rangle$ como álgebras del tipo B_1. En este caso, para $n = 1$, el lema y los enunciados $i)$ y $ii)$ son correctos de manera notoria. Si v comienza con $x_k \neq x_1$, entonces puede emplearse directamente el supuesto inductivo. Si $v = u_{1m}$, literalmente pueden repetirse los argumentos del Lema A.7, comenzando con la fórmula (A.12). Sea $v = w_{1m}$. Si $m > 2$, entonces por el Lema A.8 tenemos que $w_{1m} = [x_1\,[w_{2m}]]$. Esto brinda la posibilidad de repetir los mismos argumentos del Lema A.7 con w en lugar de u.

Consideremos el último caso en que $v = w_{12}$. Por el Lema A.8 se tiene que

$$[w_{12}] = [w_{13}]\, x_2 - p\,(w_{13}, x_2)\, x_2\, [w_{13}]\,, \tag{A.37}$$

$$[w_{13}] = x_1\, [w_{23}] - p\,(x_1, w_{23})\, [w_{23}]\, x_1. \tag{A.38}$$

$$\tag{A.39}$$

Al aplicar el coproducto primero a (A.38) y luego a (A.37) podemos hallar la suma $\sum$ para todos los tensores $w^{(1)} \otimes w^{(2)}$ de $\Delta\,([w_{12}])$ con $\deg_1\left(w^{(2)}\right) = 1$, $\deg_k\left(w^{(2)}\right) = 0$, $k > 1$ (en mucho, de la misma forma que en (A.14)):

$$\begin{aligned}\sum &= (\epsilon g_1 [w_{23}] \otimes x_1)(x_2 \otimes 1) - p(w_{13}, x_2)(x_2 \otimes 1)(\epsilon g_1 [w_{23}] \otimes x_1) \\ &= \epsilon g_1 ([w_{23}] x_2 - p(w_{13}, x_2) p(x_2, x_1) x_2 [w_{23}]) \otimes x_1. \end{aligned} \tag{A.40}$$

Para $n > 2$, tomando en cuenta primero la propiedad bicaracter de p, entonces la igualdad $[x_2 [w_{23}]] = x_2 [w_{23}] - p(x_2, w_{23}) [w_{23}] x_2$, y luego las siguientes relaciones $p_{ij}p_{ji} = 1$, $i - j > 1$; $p_{11}^{-1} = p_{12}p_{21} = p_{22}^{-1} = p_{23}p_{32}$, podemos escribir

$$\sum = \epsilon g_1 \left(-p(w_{13}, x_2) p_{21} [x_2 w_{23}] + \left(1 - p_{11}^{-1}\right) [w_{23}] \cdot x_2\right) \otimes x_1. \tag{A.41}$$

Consideremos el lado izquierdo de este tensor en la aplicación de la hipótesis inductiva. Notemos que $x_2 w_{23}$ es una palabra estándar y que $[x_2 w_{23}]$ es igual a $[x_2 [w_{23}]]$. Esta súper letra no es dura en $U_P(\mathfrak{g})$ dado que $x_2 w_{23}$ contiene la subpalabra $x_2^2 x_3$. Así, $[x_2 w_{23}]$ es una combinación lineal de súper palabras monótonas no decrecientes en menos súper letras. Entre dichas súper palabras no hay $[w_{23} \cdot x_2]$ puesto que $x_2 > x_2 w_{23}$. Por otra parte, $[w_{23}] \cdot x_2$ es una súper palabra monótona no decreciente y por consiguiente su valor en $U_P(\mathfrak{g})$ es el de un elemento base. Por ello, para $n > 2$ el lado izquierdo W de $\sum$ es distinto de cero.

Para $n = 2$, por la definición $w_{23} = x_2$, $w_{13}x_1x_2$, y la igualdad (A.40) retoma la forma $\sum = \epsilon g_1 (1 - p_{12}p_{22}p_{21}) x_2^2 \otimes x_1$. Puesto que $1 \neq p_{11}^{-1} = p_{12}p_{21} = p_{22}^{-2}$, se tiene que $(1 - p_{12}p_{22}p_{21}) = 1 - p_{22}^{-1} \neq 0$. De manera que en este caso $\sum \neq 0$ también.

Por [35, Corolario 10] y la hipótesis inductiva, la subálgebra generada por $x_2, \ldots, x_n$ tiene divisores distintos de cero. En particular, $W^h \neq 0$ y $\sum^h \neq 0$ en cualquier caso.

Resta notar que para $n > 1$ la suma de todos los tensores $w^{(1)} \otimes w^{(2)}$ de $\Delta\left([w_{12}]^h\right)$ tales que $\deg_1\left(w^{(2)}\right) = h$, $\deg_k\left(w^{(2)}\right) = 0$, $k > 1$ es igual con $\sum^h$. Por consiguiente, $[w_{12}]^h$ no puede ser primitivo torcido. □

Concluimos pues con la demostración del Teorema B_n.

Demostración del Teorema B_n. Dado que ninguna de u_{km}, w_{km} contiene subpalabras (A.1), los lemas A.16, A.1, 3.20 implican el primer enunciado.

Si $[v] \in B$ tiene altura finita, entonces por el Lema A.13 y la versión homogénea de la Definición 3.16, tenemos que $[v]^h = 0$. Para $p_{11} \neq 1$ esto contradice al Lema A.17.

En la misma línea, por el Lema 3.21, todo elemento primitivo torcido homogéneo tiene la forma $[v]^h$. Esto, junto con el Lema A.17, demuestra la cuarta afirmación y, para $p_{11} \neq 1$, también la segunda.

Si $p_{11} = 1$, entonces por (A.19) se sigue que $p_{nn}^2 = 1$, $p_{ii} = 1$, $i < n$. Además, $p_{ij}p_{ji} = 1$ para todas i, j. Esto significa que el conmutador torcido es una operación cuántica de Lie. En consecuencia, todos los elementos de B son primitivos torcidos. En el caso de $p_{nn} = 1$ estos elementos generan una álgebra de Lie coloreada, en tanto que en el caso de $p_{nn} = -1$ generan una súper álgebra de Lie coloreada. Ahora, como en el Teorema A_n, podemos hacer uso del teorema PBW para las súper álgebras de Lie coloreadas.

La tercera afirmación se sigue del Teorema 3.24 y los lemas 3.25, A.12 si se demuestra que todas las súper letras (A.17) son cero en $U_P(\mathfrak{g})$. Ya hemos probado que todas esas súper letras son no duras. Por lo tanto, queda emplear la versión homogénea de la Definición 3.15 y el Lema A.13. □

Referencias

[1] N. Andruskiewitsch and H.J. Schneider. Pointed Hopf algebras. *arXiv preprint math/0110136*, 2001.

[2] E.F. Assmus and H.F. Mattson. Coding and combinatorics. *Siam Review*, 16(3):349–388, 1974.

[3] H. Bass. K-theory and stable algebra. *Publications Mathématiques de l'IHES*, 22(1):5–60, 1964.

[4] M. Beattie, S. Dăscălescu, and Ş. Raianu. Lifting of Nichols algebras of type B_2. *Israel Journal of Mathematics*, 132(1):1–28, 2002.

[5] G.M. Bergman. The diamond lemma for ring theory. *Advances in Mathematics*, 29(2):178–218, 1978.

[6] K. Bogart, D. Goldberg, and J. Gordon. An elementary proof of the MacWilliams theorem on equivalence of codes. *Information and Control*, 37(1):19–22, 1978.

[7] L.A. Bokut'. Embeddings into simple associative algebras. *Algebra and Logic*, 15(2):73–90, 1976.

[8] A.R. Calderbank, A.R. Hammons, P.V. Kumar, N. J.A. Sloane, and P. Sole. A linear construction for certain Kerdock and Preparata codes. *American Mathematical Society*, 29(2):218–222, 1993.

[9] K.T. Chen, R.H. Fox, and R.C. Lyndon. Free differential calculus, iv. the quotient groups of the lower central series. *Annals of Mathematics*, pages 81–95, 1958.

[10] H.L. Claasen and R.W. Goldbach. A field-like property of finite rings. *Indagationes Mathematicae*, 3(1):11–26, 1992.

[11] Codility. Time complexity. Disponible en: `https://codility.com/media/train/1-TimeComplexity.pdf`, última consulta: 05/12/2014 2014.

[12] P.M. Cohn. *Universal algebra*. Springer, 1981.

[13] J. Cuadra, J.M. Garcıa-Rubira, and J.A. López-Ramos. Codes as ideals over some pointed Hopf algebras. In *Proceedings of the 19th International Symposium on Mathematical Theory of Networks and Systems–MTNS*, volume 5, 2010.

[14] J. Cuadra, J.M. García-Rubira, and J.A. López-Ramos. Determining all indecomposable codes over some Hopf algebras. *Journal of Computational and Applied Mathematics*, 235(7):1833–1839, 2011.

[15] C.W. Curtis and I. Reiner. *Representation theory of finite groups and associative algebras*, volume 356. American Mathematical Soc., 1966.

[16] M. Díaz-Sosa and V. Kharchenko. Combinatorial rank of $u_q(\mathfrak{so}_{2n})$. (En proceso), 2014.

[17] H.Q. Dinh and S.R. López-Permouth. On the equivalence of codes over finite rings. *Appliable Algebra in Engineering, Communication and Computing*, 15:37–50, 2004.

[18] V.G. Drinfeld. Quantum groups. *Zapiski Nauchnykh Seminarov POMI*, 155:18–49, 1986.

[19] O. Gabber and V. Kac. On defining relations of certain infinite-dimensional Lie algebras. *Bull. Amer. Math. Soc*, 5, 1981.

[20] M. Greferath. Orthogonality matrices for modules over finite Frobenius rings and MacWilliams' equivalence theorem. *Finite Fields and Their Applications*, 8(3):323–331, 2002.

[21] M. Greferath, A. Nechaev, and R. Wisbauer. Finite quasi-Frobenius modules and linear codes. *Journal of Algebra and its Applications*, 3(03):247–272, 2004.

[22] M. Greferath and S.E. Schmidt. Finite-ring combinatorics and MacWilliams' equivalence theorem. *Journal of Combinatorial Theory, Series A*, 92(1):17–28, 2000.

[23] A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, and P. Sole. The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes. *Information Theory, IEEE Transactions on*, 40(2):301–319, 1994.

[24] R.G. Heyneman and D.E. Radford. Reflexivity and coalgebras of finite type. *Journal of Algebra*, 28(2):215–246, 1974.

[25] Y. Hirano. On admissible rings. *Indagationes Mathematicae*, 8(1):55–59, 1997.

[26] G.P. Hochschild. *Basic theory of algebraic groups and Lie algebras*, volume 75 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1981.

[27] T. Honold. Characterization of finite Frobenius rings. *Archiv der Mathematik*, 76:406–415, 2001.

[28] H. Hopf. Über die Topologie der Gruppen-Mannigfaltigkeiten und ihre Verallgemeinerungen. *The Annals of Mathematics*, 42(1):22–52, 1941.

[29] W.C. Huffman and V. Pless. *Fundamentals of error-correcting codes*, volume 22. Cambridge University Press, 2003.

[30] V.G. Kac. *Infinite-dimensional Lie algebras*, volume 44. Cambridge University Press, 1994.

[31] M. Kashiwara. Crystalizing the q-analogue of universal enveloping algebras. *Communications in Mathematical Physics*, 133(2):249–260, 1990.

[32] M. Kashiwara. On crystal bases of the q-analogue of universal enveloping algebras. *Duke Math. Journal*, 63:465–516, 1991.

[33] V. Kharchenko and M.L. Díaz-Sosa. Computing the combinatorial rank of $u_q(\mathfrak{so}_{2n+1})$. *Communications in Algebra*, (39):4705–4718, 2011.

[34] V.K. Kharchenko. An algebra of skew primitive elements. *Algebra and Logic*, 37(2):101–126, 1998.

[35] V.K. Kharchenko. A quantum analog of the Poincaré-Birkhoff-Witt theorem. *Algebra and Logic*, 38(4):259–276, 1999.

[36] V.K. Kharchenko. Skew primitive elements in Hopf algebras and related identities. *Journal of Algebra*, 238(2):534–559, 2001.

[37] V.K. Kharchenko. A combinatorial approach to the quantification of Lie algebras. *Pacific Journal of Mathematics*, 203(N1):191–233, 2002.

[38] V.K. Kharchenko. Constants of coordinate differential calculi defined by Yang–Baxter operators. *Journal of Algebra*, 267(1):96–129, 2003.

[39] V.K. Kharchenko. PBW-bases of coideal subalgebras and freeness theorem. *Transactions of the American Mathematical Society*, 360(10):5121–5143, 2008.

[40] V.K. Kharchenko. Triangular decomposition of right coideal subalgebras. *Journal of Algebra*, 324(11):3048–3089, 2010.

[41] V.K. Kharchenko. Right coideal subalgebras in $u_q^+(\mathfrak{so}_{2n+1})$. *Journal of the European Mathematical Society*, 13(N6):1677–1735, 2011.

[42] V.K. Kharchenko and A. Andrade-Álvarez. On the combinatorial rank of Hopf algebras. *Contemporary Mathematics*, 376:299, 2005.

[43] V.K. Kharchenko and A.V. Lara-Sagahon. Right coideal subalgebras in $U_q(\mathfrak{sl}_{n+1})$. *Journal of Algebra*, 319:2571–2625, 2007.

[44] A.N. Koryukin. Simplest algebraic dependencies of skew derivations of prime rings. *Algebra and Logic*, 36:407–421, 1997.

[45] T.Y. Lam. *Lectures on modules and rings*. Number 189. Springer, 1999.

[46] T.Y. Lam. *A first course in noncommutative rings*. Springer Science & Business, 2013.

[47] R.G. Larson and M. Sweedler. An associative orthogonal bilinear form for Hopf algebras. *American Journal of Mathematics*, 91:75–93, 1969.

[48] M. Lothaire. Combinatorics on Words, volume 17 of Encyclopedia of Mathematics and its Applications, 1983.

[49] M. Lothaire. *Algebraic combinatorics on words*. Cambridge University Press, 2002.

[50] F.J. MacWilliams. Error-correcting codes for multiple-level transmission. *Bell System Technical Journal*, 40(1):281–308, 1961.

[51] F.J. MacWilliams. Combinatorial properties of elementary abelian groups. *Radcliffe College, Cambridge*, 1962.

[52] F.J. MacWilliams and N.J.A. Sloane. *The theory of error-correcting codes*, volume 16. Elsevier, 1977.

[53] A. Milinski and H.J. Schneider. Pointed indecomposable Hopf algebras over Coxeter groups. *Contemporary Mathematics*, 267:215–236, 2000.

[54] S. Montgomery. *Hopf algebras and their actions on rings*. Number 82. American Mathematical Society, 1993.

[55] E. Müller. Some topics on Frobenius–Lusztig kernels, I. *Journal of Algebra*, 206(2):624–658, 1998.

[56] V. Pless and Z. Qian. Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$. *Information Theory, IEEE Transactions on*, 42(5):1594–1600, 1996.

[57] V. Pless, P. Solé, and Z. Qian. Cyclic self-dual $\mathbb{Z}_4$-codes. *Finite Fields and Their Applications*, 3(1):48–69, 1997.

[58] D.E. Radford. Hopf algebras with projection. *Journal of Algebra*, 92:322–347, 1985.

[59] D.E. Radford. The structure of Hopf algebras with a projection. *Journal of Algebra*, 92(2):322–347, 1985.

[60] W.F. Santos and A. Rittatore. *Actions and invariants of algebraic groups*. CRC Press, 2010.

[61] J.P. Serre and L.L. Scott. *Linear representations of finite groups*, volume 42. Springer, 1977.

[62] C.E. Shannon. A mathematical theory of communication. *ACM SIGMOBILE Mobile Computing and Communications Review*, 5(1):3–55, 2001.

[63] A.I. Shirshov. On Free Lie Rings. In *Selected Works of A.I. Shirshov*, pages 77–87. Springer, 2009.

[64] A.I. Shirshov. Some algorithmic problems for Lie algebras. In *Selected Works of A.I. Shirshov*, pages 125–130. Springer, 2009.

[65] A.I. Shirshov. Subalgebras of Free Lie Algebras. In *Selected Works of AI Shirshov*, pages 3–13. Springer, 2009.

[66] J.B. Sullivan. The uniqueness of integrals for Hopf algebras and some existence theorems of integrals for commutative Hopf algebras. *Journal of Algebra*, 19(3):426–440, 1971.

[67] J.B. Sullivan. A decomposition theorem for pro-affine solvable algebraic groups over algebraically closed fields. *American Journal of Mathematics*, 95(1):221–228, 1973.

[68] M.E. Sweedler. *Hopf algebras*, volume 202. WA Benjamin New York, 1969.

[69] E.J. Taft and R.L. Wilson. On antipodes in pointed Hopf algebras. *Journal of Algebra*, 29(1):27–32, 1974.

[70] M. Takeuchi. Free Hopf algebras generated by coalgebras. *Journal of the Mathematical Society of Japan*, 23(4):561–582, 1971.

[71] M. Takeuchi. On a semi-direct product decomposition of affine groups over a field of characteristic 0. *Tohoku Mathematical Journal*, 24(3):453–456, 1972.

[72] M. Takeuchi. Survey of braided Hopf algebras. *Contemporary Mathematics*, 267:301–324, 2000.

[73] A. Terras. *Fourier analysis on finite groups and applications*. Number 43. Cambridge University Press, 1999.

[74] H. Ward and J.A. Wood. Characters and the equivalence of codes. *Journal of Combinatorial Theory, Series A*, 73(2):348–352, February 1996.

[75] J.A Wood. A coding-theoretic characterization of finite Frobenius rings. Disponible en: `http://homepages.wmich.edu/~jwood/eprints/characterization.pdf`, última consulta: 21/11/2014.

[76] J.A. Wood. Extension theorems for linear codes over finite rings. *Lecture Notes in Computer Science*, 1255:329–340, 1997.

[77] J.A. Wood. Duality for modules over finite rings and applications to coding theory. *American Journal of Mathematics*, 121(3):555–575, 1999.

[78] J.A. Wood. Code equivalence characterizes finite Frobenius rings. *Proceedings of the American Mathematical Society*, 136(2):699–706, 2008.

[79] J.A. Wood. Foundations of linear codes defined over finite modules: the extension theorem and the MacWilliams identities. *Codes Over Rings (Ankara, 2008), Ser. Coding Theory Cryptol.*, 6:124–190, 2009.

[80] J.A. Wood. Applications of finite Frobenius rings to the foundations of algebraic coding theory. In *44th Symposium on Rings and Representation Theory Japan*, 2011.

[81] X. Xiaoping. Representations of lie algebras and coding theory. arXiv:0902.2837v2, 2009.