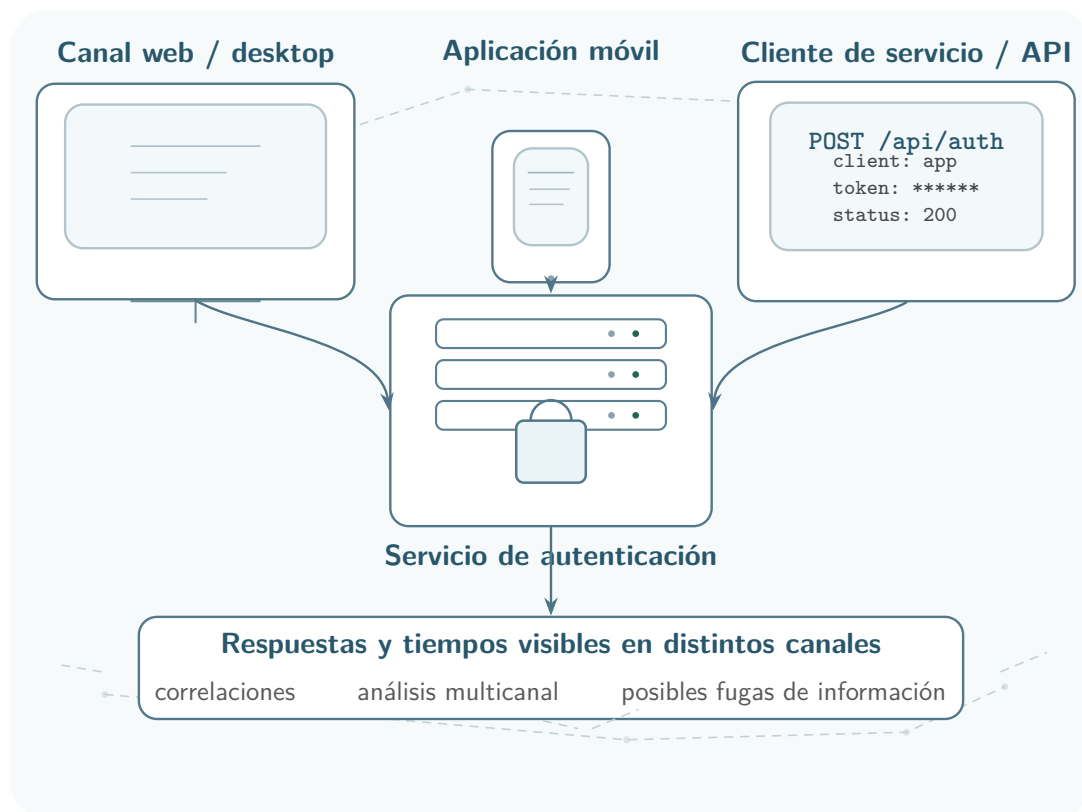


Correlaciones y fugas de información en la autenticación web

Un enfoque basado en Exact Centered Gram Synthesis



Hugo Vázquez Caramés

hvaquez@pentest.es

29 Septiembre de 2026

Resumen

La privacidad de un sistema de autenticación depende también de lo que revela su comportamiento. El tiempo de respuesta, por ejemplo, puede transmitir información sobre procesos internos. Cuando una aplicación ofrece varias vías de acceso, como una página web y una aplicación móvil, aparece una dimensión adicional: la relación entre sus respuestas.

Dos conjuntos de observaciones pueden tener las mismas distribuciones individuales y diferir en su comportamiento conjunto. Este informe desarrolla un marco teórico para estudiar esa estructura mediante **Exact Centered Gram Synthesis**, o **ECGS**, que puede traducirse como síntesis exacta de Gram centrada. La construcción compara un operador con una referencia calibrada, representa la diferencia mediante una forma positiva y conserva los términos cruzados al combinar las contribuciones. Su interés para la seguridad consiste en organizar el análisis de las dependencias y orientar la evaluación defensiva de posibles fugas de información.

1 La información contenida en las relaciones

Una aplicación puede mostrar el mismo mensaje de error y realizar un trabajo interno diferente en cada caso. Parte de ese trabajo puede reflejarse en el tiempo que tarda en responder. Cuando una característica observable permite obtener información que debía permanecer protegida, existe un canal lateral.

El comportamiento de una aplicación incluye tanto las respuestas individuales como sus relaciones. Una página web y una aplicación móvil pueden utilizar servicios internos comunes. La carga de esos servicios, la gestión de sesiones o el acceso a recursos compartidos pueden influir en ambas vías. Por eso, la descripción de cada una por separado deja abierta una pregunta: ¿cómo se comportan cuando se consideran conjuntamente?

La figura 1 muestra el recorrido conceptual desde las respuestas de los distintos canales hasta su representación conjunta mediante ECGS.

Para ver la idea de forma más directa, comparemos cuatro intentos de acceso observados al mismo tiempo en dos canales: web y móvil. En las dos situaciones, cada canal responde dos veces rápido y dos veces lento. Lo que cambia no es el recuento de cada canal por separado, sino la forma en que ambos se coordinan.

La figura muestra por qué mirar cada canal por separado puede ser insuficiente. En ambas situaciones, web y móvil presentan exactamente dos respuestas rápidas y dos lentas. Sin embargo, en la segunda situación existe una coordinación perfecta entre ambos canales. Esa coordinación es información adicional que no aparece en los recuentos individuales.

En una aplicación, esa relación podría reflejarse en variaciones coordinadas de los tiempos de respuesta. La correlación describe una parte de esta estructura: la tendencia de dos magnitudes a variar de forma relacionada. También pueden existir dependencias más complejas, por lo que una descripción estadística completa comprende tanto las distribuciones individuales como la distribución conjunta.

La relevancia para la seguridad aparece cuando una diferencia observable está vinculada con información protegida. La arquitectura y las condiciones de funcionamiento proporcionan el contexto para interpretar ese vínculo. Una fluctuación de carga y una diferencia asociada a un proceso sensible pueden producir señales parecidas; su significado se establece al relacionar las observaciones con el funcionamiento del sistema.

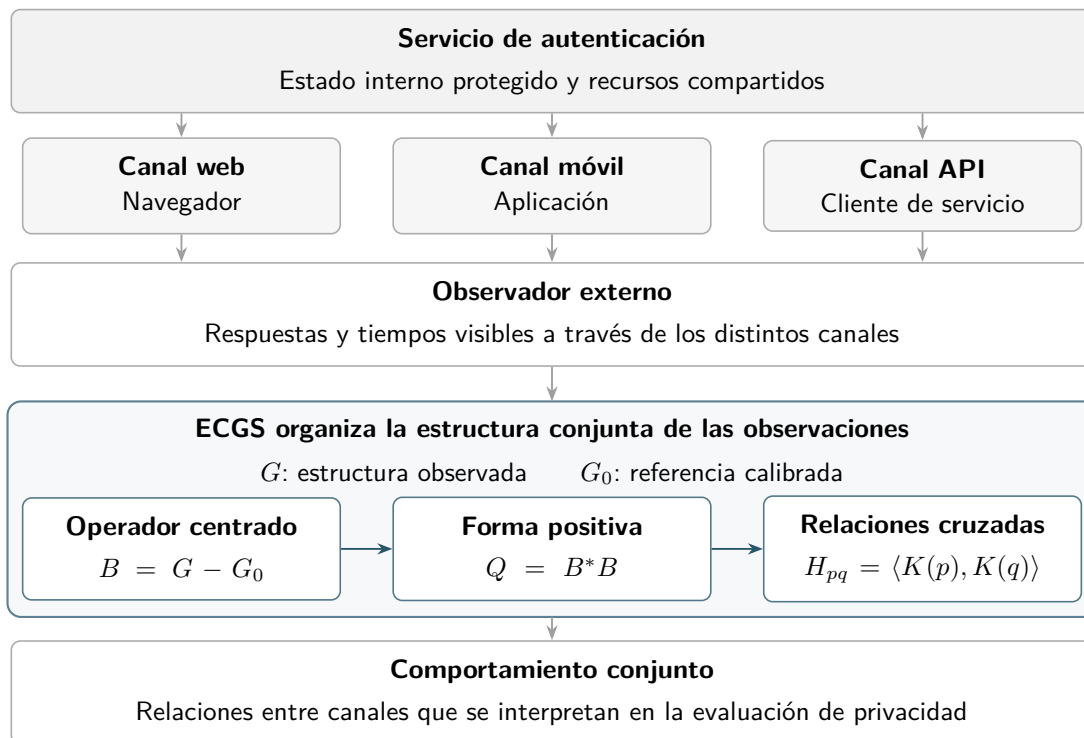


Figura 1: Canal lateral multicanal y representación mediante ECGS. La posible fuga reside en la dependencia entre el comportamiento observable y la información protegida. ECGS conserva las relaciones incluidas en el modelo para estudiar ese comportamiento de forma conjunta.

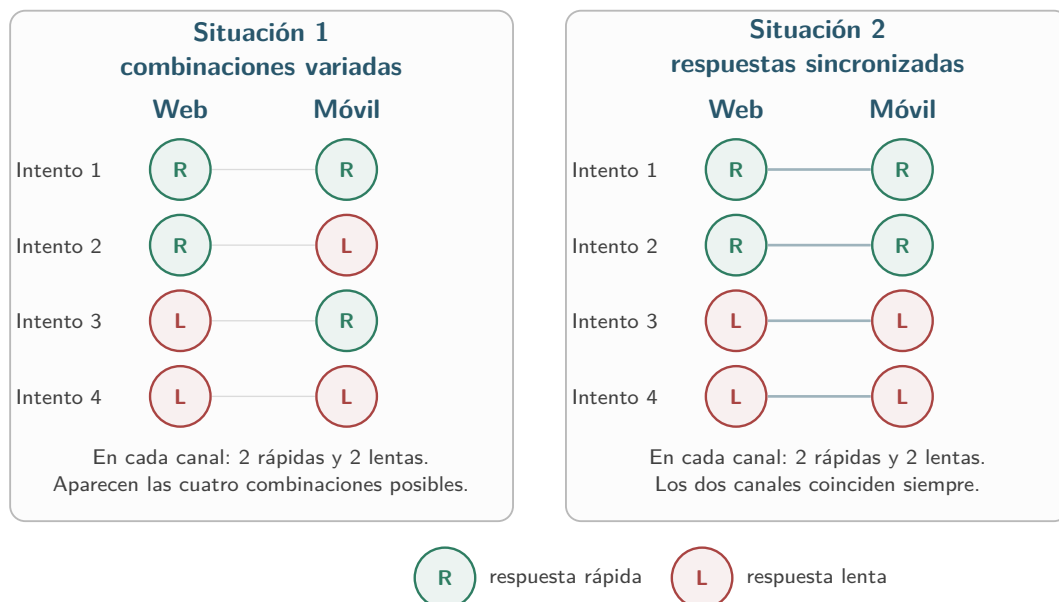


Figura 2: Dos situaciones con el mismo reparto individual de respuestas y una relación distinta entre los canales. En la situación 1 aparecen todas las combinaciones; en la situación 2, web y móvil se mueven siempre a la vez. Esta figura es una simplificación de la realidad con fines educativos.

2 Origen del enfoque

La inspiración matemática de este trabajo procede del manuscrito sobre una estimación de densidad de ceros de la función zeta de Riemann de la referencia [1]. La exposición de su cadena de demostración, recogida en [2], permite localizar la construcción de síntesis exacta en el apartado denominado «Step 7». La idea que se toma de esa construcción es formar un objeto a partir de sus contribuciones indexadas y conservar sus relaciones al desarrollar la expresión cuadrática correspondiente.

En términos sencillos, se combinan primero las contribuciones con sus pesos y después se calcula la magnitud del conjunto. Al efectuar ese cálculo aparecen productos entre contribuciones distintas. Esos productos cruzados describen cómo se refuerzan o se compensan unas con otras.

El manuscrito dedicado a radar e imagen coherente [3] formula ECGS para datos multicanal: se resta una referencia calibrada a un operador de Gram o de covarianza, se construye una forma positiva a partir del residuo y se asocian vectores a los índices físicos de la tarea. Esta formulación proporciona el punto de partida del desarrollo que sigue.

En el contexto de la autenticación, las magnitudes observadas pueden ser reales, como los tiempos de respuesta. La formulación admite también números complejos, lo que permite expresar en un mismo lenguaje las identidades generales de ECGS. Aquí, la interpretación se centra en la organización de las variaciones y de los términos cruzados. El nombre «síntesis exacta» designa la igualdad algebraica entre las distintas expresiones de una misma construcción.

3 Interpretación intuitiva del procedimiento

Los apartados matemáticos trasladados al anexo formalizan cinco ideas que pueden explicarse sin recurrir a matrices ni a fórmulas. Esta sección ofrece una interpretación equivalente para lectores sin formación matemática. Las comparaciones que siguen son **analogías**: sirven para explicar la función de cada paso, no sustituyen a su definición matemática, que se conserva literalmente en el anexo.

3.1 Observar no solo cada canal, sino también cómo se relacionan

El primer paso consiste en resumir qué suele ocurrir en cada canal y cuánto se aparta de ese comportamiento habitual. Pero el análisis no termina ahí: también se registra si los cambios de un canal aparecen al mismo tiempo que los de otro. Así, dos sistemas pueden parecer idénticos si se estudian web, móvil y API por separado y, sin embargo, ser muy distintos cuando se observa la relación entre ellos.

Analogía. Pensemos en tres ascensores de un edificio. Saber cuánto tarda, en promedio, cada ascensor es útil, pero no dice si los tres se retrasan siempre a la vez. Si los retrasos coinciden, probablemente exista una causa compartida, por ejemplo una sobrecarga eléctrica o un sistema de control común. El análisis multicanal busca precisamente ese tipo de información adicional.

3.2 Comparar el comportamiento real con una referencia estable

Después se fija una referencia: una descripción del sistema cuando funciona en unas condiciones conocidas y consideradas normales. El comportamiento observado se compara con esa referencia para identificar qué ha cambiado. La comparación debe hacerse con datos contruidos de la misma

forma y bajo condiciones compatibles; de otro modo, una diferencia podría deberse simplemente a que se están comparando cosas distintas.

El método conserva dos ideas a la vez: *cuánto* se ha separado el sistema de la referencia y *en qué sentido* se ha producido ese cambio. Esto permite distinguir entre una desviación pequeña y una grande, y también entre cambios que, aunque tengan un tamaño parecido, afectan de manera distinta a los canales.

Analogía. Es como colocar una fotografía actual sobre una plantilla transparente tomada cuando todo funcionaba correctamente. La distancia entre ambas permite ver cuánto ha cambiado la escena; además, la dirección de cada desplazamiento indica qué elementos se han movido y hacia dónde.

3.3 Combinar las señales sin perder sus interacciones

Cada canal, condición o tipo de observación puede aportar una contribución al resultado final. ECGS combina esas contribuciones, pero evita tratarlas como si fueran piezas independientes. Conserva también las relaciones entre cada par de contribuciones, porque dos señales pueden reforzarse mutuamente, compensarse o aparecer coordinadas.

Esta es una parte central del enfoque: el resultado final no depende solo de la intensidad de cada elemento por separado, sino también de cómo encaja con los demás. Al mantener esas relaciones es posible seguir qué interacciones explican una desviación observada.

Analogía. Una orquesta no se describe correctamente midiendo por separado el volumen de cada instrumento. Dos instrumentos pueden tocar la misma nota y reforzarse, o producir efectos que se compensan. Escuchar el conjunto exige conservar tanto la aportación de cada instrumento como la relación entre ellos.

3.4 Ordenar muchas relaciones sin alterar el resultado

Cuando hay numerosos canales, momentos o condiciones, el número de relaciones puede crecer rápidamente. El procedimiento permite agruparlas según un criterio útil, por ejemplo por tipo de canal, distancia temporal o procedencia, sin perder ninguna contribución y sin modificar el resultado total. La agrupación cambia la forma de presentar el análisis, no la información que contiene.

Esto facilita localizar patrones: en vez de inspeccionar una lista enorme de interacciones individuales, se pueden estudiar familias de relaciones y ver qué grupos concentran los efectos más relevantes o qué grupos se compensan entre sí.

Analogía. Es como ordenar todas las operaciones de una empresa en carpetas, por ejemplo ventas, proveedores, nóminas y transporte. El balance total sigue siendo el mismo; lo que cambia es que ahora resulta más fácil identificar de dónde procede cada parte del resultado.

3.5 Distinguir variaciones independientes de causas compartidas

El último paso interpretativo consiste en preguntar qué tipo de mecanismo podría producir las relaciones observadas. A veces cada canal contiene su propio ruido, pero existe además una causa común que afecta a varios a la vez: carga del servidor, acceso a una base de datos compartida, gestión de sesiones o cualquier otro recurso común. En ese caso, parte de la variación aparece coordinada.

También puede ocurrir algo más sutil: cada canal, estudiado aisladamente, mantiene exactamente el mismo comportamiento estadístico, pero cambia la manera en que se coordina con los demás. El ejemplo gráfico de la figura 2 muestra justamente esa posibilidad: dos rápidas y dos lentas en cada canal en ambos casos, pero una dependencia conjunta diferente.

Analogía. Dos personas pueden abrir el paraguas dos veces cada una durante una mañana. Ese recuento individual es el mismo tanto si lo hacen en momentos independientes como si siempre lo abren simultáneamente porque están reaccionando a la misma lluvia. El número de aperturas no revela por sí solo la existencia de una causa compartida; la sincronización sí aporta esa pista.

En conjunto, estos cinco pasos convierten las observaciones multicanal en una descripción estructurada: se caracteriza cada canal, se compara con una referencia, se conservan las interacciones, se organizan esas interacciones y se interpreta si existe una variación compartida. La formulación exacta de estas ideas se recoge en el anexo de interpretación matemática.

4 La evaluación de seguridad como estudio del comportamiento conjunto

En una evaluación defensiva, la pregunta central es si las observaciones disponibles revelan información que el sistema debe proteger. El modelo multicanal aporta una forma de describir esas observaciones y sus relaciones. ECGS proporciona, dentro de ese estudio, una representación cuya referencia, contribuciones y términos cruzados quedan definidos de manera explícita.

La interpretación combina la descripción estadística con el conocimiento de la arquitectura. La carga del servidor, la red y los recursos compartidos forman parte del contexto, porque pueden explicar variaciones coordinadas. La estabilidad de un patrón en distintos periodos y condiciones ayuda a valorar su alcance. La estimación de la incertidumbre acompaña a cualquier conclusión obtenida a partir de mediciones.

La utilidad práctica de una representación se evalúa en función de una tarea y un criterio definidos. Una comparación informativa utiliza los mismos datos, condiciones de calibración y recursos de cálculo para ECGS y para los métodos de referencia. Los datos empleados para valorar el resultado se mantienen separados de los utilizados para ajustar las decisiones del análisis. Este planteamiento permite atribuir una mejora observada a la representación o al estimador correspondiente.

Desde el diseño del sistema, la protección comprende el mensaje visible y el comportamiento del procesamiento. OWASP recomienda respuestas de autenticación genéricas y advierte de las diferencias reveladoras en tiempos y códigos de respuesta. [4] La perspectiva multicanal extiende esa atención a las relaciones entre las vías de acceso y a los recursos que comparten.

El objetivo de ingeniería es reducir la dependencia observable respecto de la información protegida. Ello orienta la revisión de los caminos de ejecución sensibles y de las decisiones internas que se reflejan en las respuestas. Las medidas de protección se valoran por el comportamiento que producen en conjunto y por su consistencia a lo largo del funcionamiento del servicio.

ECGS ofrece una formulación para investigar esa dimensión de la privacidad: una referencia describe el contexto, el operador centrado representa la desviación y la síntesis conserva las relaciones incluidas en el modelo. El desarrollo presentado establece las identidades matemáticas de esa representación. Su rendimiento en autenticación constituye una cuestión experimental que requiere mediciones y comparación con métodos establecidos.

5 Prompt de ejemplo para el desarrollo de una herramienta asistida por LLM

A continuación se incluye un ejemplo de prompt inicial pensado para iniciar un proceso interactivo entre un modelo de lenguaje y un experto en ciberseguridad con el objetivo de terminar construyendo una herramienta funcional capaz de observar anomalías en procesos de autenticación multicanal. Debido a la complejidad matemática del enfoque, se recomienda utilizar un LLM de última generación y, si el proyecto no es confidencial, preferiblemente un modelo frontera. Si se usa un modelo local, conviene elegir el que tenga mejores capacidades matemáticas, sin confundirlas con simples capacidades de programación.

Actúa como arquitecto de investigación y desarrollo para una herramienta de análisis de canal lateral en autenticación multicanal. Debes trabajar de forma interactiva conmigo, que actuaré como experto en ciberseguridad y conocimiento del sistema objetivo. Tu tarea es ayudarme a transformar el contenido de este informe y de sus referencias en una tool funcional que permita observar anomalías en procesos de autenticación web, móvil y API, con especial atención a correlaciones, dependencias conjuntas y posibles fugas de información a través de tiempos de respuesta, patrones de error, códigos de respuesta y cualquier otra señal observable.

Usa este documento como base conceptual principal y utiliza también sus referencias para reconstruir con rigor el marco matemático, el contexto de seguridad y los posibles caminos de implementación. No des por supuesto que el objetivo está completamente especificado: debes guiar una conversación estructurada para completar requisitos, refinar hipótesis, delimitar el alcance y llegar a un diseño implementable.

Quiero que conduzcas el proceso por fases. En cada fase debes pedirme la información mínima necesaria, explicar por qué la necesitas y producir entregables concretos antes de pasar a la siguiente fase. Las fases deben incluir, como mínimo: comprensión del problema; definición del caso de uso defensivo; inventario de canales y observables; diseño del modelo de datos; selección de métricas y señales; traducción operativa del enfoque ECGS; diseño experimental; estrategia de detección de anomalías; arquitectura software; plan de validación; plan de despliegue; consideraciones de privacidad, cumplimiento y seguridad; y hoja de ruta de implementación.

Necesito que conviertas el contenido matemático en decisiones de ingeniería accionables. Cuando introduces una idea matemática, explica de inmediato cómo se traduce a estructuras de datos, transformaciones, cálculos, visualizaciones, criterios de alerta o módulos software. Si existe ambigüedad entre varias interpretaciones razonables, compáralas y proponme cómo decidir entre ellas con experimentos.

Quiero que el resultado final desemboque en una herramienta funcional. Por tanto, debes acabar proporcionando: 1) especificación funcional completa; 2) arquitectura técnica; 3) esquema de ingesta de datos; 4) diseño de pipeline analítico; 5) definición de métricas, umbrales e indicadores; 6) propuesta de interfaz o panel de observación; 7) pseudocódigo o código base de los módulos principales; 8) plan de pruebas con datos sintéticos y reales; 9) criterios para interpretar hallazgos sin sobredimensionarlos; y 10) lista de riesgos y limitaciones.

No avances demasiado deprisa. Empieza preguntándome por el contexto operativo concreto, los canales de autenticación disponibles, los logs o mediciones a los que tendríamos acceso, el volumen de datos esperado, las restricciones legales y de confidencialidad, y el lenguaje o stack en el que preferiríamos implementar la tool. Después de mis respuestas, mantén siempre una dinámica iterativa y acumulativa hasta completar un diseño que pueda implementarse de forma realista.

Anexo: interpretación matemática

En este anexo se muestra el desarrollo matemático que fundamenta el ataque.

A Representación matemática de las observaciones

Consideremos un vector Y con m componentes, cada una asociada a una magnitud observada. Trabajaremos sobre $\mathbb{F} = \mathbb{R}$ o $\mathbb{C}$, con segundos momentos finitos. El símbolo $*$ representa la traspuesta conjugada; para datos reales se reduce a la traspuesta. El producto interno se define mediante $\langle u, v \rangle = u^*v$.

La media y la matriz de covarianza son

$$\mu = \mathbb{E}[Y], \quad C = \mathbb{E}[(Y - \mu)(Y - \mu)^*].$$

La media describe el nivel habitual de cada componente. La diagonal de C recoge sus varianzas, es decir, la amplitud de las fluctuaciones alrededor de la media. Las entradas fuera de la diagonal recogen las covarianzas entre componentes. En el caso real, su signo indica si las variaciones tienden a acompañarse o a producirse en sentidos opuestos.

Las covarianzas dependen de las unidades empleadas. Cuando interesa una escala adimensional y todas las varianzas son positivas, se utiliza la matriz de correlación

$$D = \text{diag}(C_{11}, \dots, C_{mm}), \quad R = D^{-1/2}CD^{-1/2}.$$

Así, C conserva la escala de las fluctuaciones y R expresa sus relaciones normalizadas. La elección entre ambas depende de la pregunta que se quiera estudiar. Una componente de varianza nula se trata por separado para que la normalización esté bien definida.

También es posible describir los datos respecto de un nivel de referencia μ_0 . En ese caso,

$$\mathbb{E}[(Y - \mu_0)(Y - \mu_0)^*] = C + (\mu - \mu_0)(\mu - \mu_0)^*.$$

La expresión reúne dos efectos: la variación alrededor de la media actual y el desplazamiento de esa media respecto de la referencia. Esta identidad permite precisar qué contiene el operador elegido antes de comparar situaciones. El centrado de las observaciones y la resta de un operador de referencia son operaciones distintas, y cada una tiene una función explícita en el modelo.

B Una referencia para describir el cambio

Sean G y G_0 dos matrices hermíticas de tamaño $m \times m$, expresadas en las mismas coordenadas y con unidades compatibles. La primera representa la estructura que se estudia y la segunda una referencia calibrada. Ambas pueden ser matrices de covarianza o matrices de Gram construidas mediante una misma regla.

La calibración fija qué comportamiento se toma como referencia y bajo qué condiciones se ha obtenido. Cuando los operadores proceden de mediciones, su interpretación incorpora la variabilidad de esas mediciones. La comparación adquiere así un significado concreto: describir la desviación respecto de un comportamiento de referencia definido.

El operador centrado y la forma positiva de ECGS se escriben como

$$B = G - G_0, \quad Q = B^* B.$$

La resta conserva la estructura de la desviación. La construcción de Q permite medir su acción mediante una cantidad no negativa: para cualquier vector u ,

$$u^* Q u = \|Bu\|^2 \geq 0.$$

Por tanto, Q es hermítica y semidefinida positiva. Como B es hermítica en esta formulación, también se cumple $Q = B^2$. La magnitud $u^* Q u$ expresa cuánto transforma B la dirección representada por u .

Una medida global del tamaño de la desviación es

$$\text{tr}(Q) = \|B\|_F^2 = \sum_{c,d=1}^m |B_{cd}|^2.$$

Aquí, $\|B\|_F$ es la norma de Frobenius. Su cuadrado suma las magnitudes al cuadrado de todas las entradas de B . Las contribuciones diagonales y las situadas fuera de la diagonal quedan incluidas en una misma expresión.

La forma Q describe magnitudes cuadráticas de la desviación; el operador B conserva además su orientación. Por ejemplo, B y $-B$ producen el mismo Q . Mantener ambos objetos permite distinguir entre el tamaño de un cambio y el sentido que tiene respecto de la referencia.

C Síntesis exacta y núcleo de Gram

Sea $\mathcal{P}$ un conjunto finito de índices. Cada índice p identifica una contribución y conserva su procedencia dentro del modelo. A él se asocian un vector $v_p \in \mathbb{F}^m$ y un peso no negativo $\omega(p)$. Con un mismo operador B para toda la construcción, definimos

$$K(p) = \sqrt{\omega(p)} B v_p.$$

Los vectores $K(p)$ expresan las contribuciones después de aplicar el operador centrado. Dados unos coeficientes $x_p \in \mathbb{F}$, su síntesis es

$$z = \sum_{p \in \mathcal{P}} x_p K(p).$$

La matriz de Gram de esta familia recoge todos sus productos internos. Sus entradas son

$$H_{pq} = \langle K(p), K(q) \rangle = \sqrt{\omega(p)\omega(q)} v_p^* Q v_q.$$

Esta matriz constituye el núcleo de la representación: la diagonal describe la magnitud de cada vector y las demás entradas describen sus relaciones geométricas. El producto interno expresa una relación algebraica entre los vectores construidos; su significado estadístico depende de cómo se hayan definido esos vectores y sus pesos.

Si V es la matriz cuyas columnas son $\sqrt{\omega(p)} v_p$ y x reúne los coeficientes, las identidades anteriores adoptan una forma compacta:

$$z = BVx, \quad H = V^*QV, \quad \|z\|^2 = x^*Hx.$$

La última igualdad se obtiene sustituyendo $z = BVx$ y usando $Q = B^*B$. También muestra que H es semidefinida positiva, porque $x^*Hx = \|BVx\|^2 \geq 0$ para cualquier x .

Al desarrollar la expresión cuadrática aparece la identidad de síntesis

$$\|z\|^2 = \sum_{p,q \in \mathcal{P}} \bar{x}_p x_q H_{pq}.$$

Fijado un orden en $\mathcal{P}$, puede separarse en contribuciones individuales y cruzadas:

$$\|z\|^2 = \sum_p |x_p|^2 \|K(p)\|^2 + 2 \operatorname{Re} \sum_{p < q} \bar{x}_p x_q H_{pq}.$$

El segundo sumando conserva la interacción entre contribuciones distintas. Su valor puede ser positivo o negativo: unas contribuciones se refuerzan y otras se compensan. Si dos vectores iguales se combinan con coeficientes opuestos, su suma se anula. Ese comportamiento forma parte de la geometría del conjunto y queda recogido por los términos cruzados.

El interés de esta expresión es poder seguir cada relación hasta el cálculo final. Para unas entradas fijadas, la síntesis directa y el desarrollo mediante H representan la misma cantidad. La elección de G_0 , de los vectores y de los pesos determina qué estructura de los datos queda representada.

D Organización de los términos cruzados

Una representación multicanal puede contener muchas contribuciones. Para estudiarlas por grupos se introduce una función $h : \mathcal{P} \times \mathcal{P} \rightarrow \mathcal{L}$, donde cada par ordenado (p, q) pertenece a una única clase ℓ . Definimos

$$E_\ell = \sum_{h(p,q)=\ell} \bar{x}_p x_q H_{pq}, \quad \|z\|^2 = \sum_{\ell \in \mathcal{L}} E_\ell.$$

La igualdad se sigue de una partición de la suma: cada término aparece exactamente una vez. Las clases permiten ordenar el cálculo según una relación entre índices y conservar el valor total de la síntesis. Los sumandos E_ℓ son contribuciones algebraicas; en el caso complejo pueden ser complejos, aunque su suma sea real y no negativa.

Cuando cada clase es estable al intercambiar p y q , los términos conjugados quedan agrupados y su contribución es real. En una indexación por enteros, la elección $h(p, q) = p - q$ reúne términos por diferencias de índice. Entonces,

$$E_{-\ell} = \overline{E_\ell}.$$

Las clases opuestas pueden reunirse mediante su parte real. Esta organización hace visible la simetría hermitica de la matriz de Gram y permite conservar las compensaciones que intervienen en la suma.

Otra identidad útil aparece cuando las contribuciones tienen índices multiplicativos. Para dos familias de coeficientes b_r y c_s con soporte finito, se define

$$x_N = \sum_{rs=N} b_r c_s, \quad \sum_N x_N K(N) = \sum_{r,s} b_r c_s K(rs).$$

Cada coeficiente x_N reúne todas las parejas cuyo producto es N . La fórmula expresa dos maneras de organizar una misma síntesis, siempre que $K(rs)$ dependa del producto y se utilice la misma familia de vectores. Cuando la procedencia de cada factor forma parte del modelo, se conserva el índice completo (r, s) .

Estas identidades permiten adaptar la organización del cálculo a la estructura de los índices. En aritmética exacta, las expresiones equivalentes dan el mismo resultado. La propiedad que se conserva es el núcleo construido y la suma definida a partir de él.

E Modelos de variación compartida

Un modelo elemental ayuda a interpretar la presencia de relaciones entre componentes. Consideremos el vector real

$$Y = \mu + \varepsilon + aZ,$$

donde ε representa fluctuaciones de fondo, Z es una perturbación escalar compartida y a indica cuánto influye esa perturbación en cada componente. Supongamos medias nulas para ε y Z , segundos momentos finitos y ausencia de correlación entre ambos. Si $\text{Cov}(\varepsilon) = \Sigma_\varepsilon$ y $\text{Var}(Z) = \tau^2$, entonces

$$\mathbb{E}[Y] = \mu, \quad \text{Cov}(Y) = \Sigma_\varepsilon + \tau^2 aa^\top.$$

La contribución compartida tiene una estructura explícita. Entre dos componentes c y d aporta $\tau^2 a_c a_d$ a la covarianza. En cada componente aporta $\tau^2 a_c^2$ a la varianza. Una misma perturbación puede manifestarse, por tanto, en la variabilidad individual y en la relación entre componentes.

También existen modelos donde las distribuciones individuales permanecen iguales y toda la diferencia se encuentra en la dependencia. Un ejemplo lo proporcionan los vectores gaussianos bidimensionales

$$X_0 \sim \mathcal{N}(0, I_2), \quad X_1 \sim \mathcal{N}\left(0, \begin{pmatrix} 1 & \rho \\ \rho & 1 \end{pmatrix}\right), \quad 0 < |\rho| < 1.$$

En ambos casos, cada componente tiene distribución normal estándar. En X_0 son independientes; en X_1 tienen correlación ρ . Las matrices son definidas positivas bajo la condición indicada. Este ejemplo da una formulación precisa de la idea ilustrada por la figura 2: las mismas distribuciones marginales pueden corresponder a comportamientos conjuntos diferentes.

Los dos modelos describen estructuras distintas. El primero representa un factor compartido que modifica varianzas y covarianzas. El segundo aísla un cambio de dependencia manteniendo las distribuciones individuales. Elegir un modelo equivale a especificar qué cambios se consideran y qué rasgos se mantienen.

Referencias

- [1] Vázquez Caramés, Hugo. *A Zero-Density Estimate with Coefficient $24000/10451 < 30/13$ for the Riemann Zeta-Function*. Manuscrito, 2026. [Consultar el manuscrito en ResearchGate](#).
- [2] Vázquez Caramés, Hugo. *Proof Chain for the $24000/10451$ Zero-Density Bound (Friendly Version)*. Manuscrito, 2026. [Consultar la exposición de la cadena de demostración en ResearchGate](#).
- [3] Vázquez Caramés, Hugo. *Toward Higher Precision in Radar and Coherent Imaging: Exact Centered Gram Synthesis for Multichannel Signals*. Manuscrito, 2026. [Consultar el manuscrito sobre ECGS en ResearchGate](#).
- [4] OWASP. *Authentication Cheat Sheet*, apartado sobre respuestas de autenticación. [Consultar la guía](#).

Nota sobre autoría y origen del documento

En la elaboración de este documento se ha utilizado un modelo de lenguaje de gran tamaño, conocido por las siglas LLM. Hugo Vázquez Caramés, autor del informe, se hace responsable de la totalidad de su contenido.

Este documento se inspira en una técnica empleada en el manuscrito matemático enlazado en la referencia [1], que en su momento superó el primer filtro editorial de la revista matemática *The Ramanujan Journal*. En este primer filtro normalmente se somete el manuscrito a revisión automatizada por parte de sistemas LLM para buscar inconsistencias de tipo técnico y además un revisor humano, un matemático de reputación mundial, realiza una valoración sobre el interés desde el punto de vista editorial.

Sin embargo, el manuscrito no se envió a revisión por pares porque, según la editorial, la nueva cota de densidad de ceros $24000/10451$ no era lo suficientemente relevante como para iniciar un proceso de revisión por pares de un documento tan extenso, algo que, por otra parte, era totalmente comprensible. En el momento de publicación de este documento el manuscrito de la referencia [1] está siendo formalizado con Lean, por lo que es posible que cuando leas esto ya esté finalizado. Puedes consultar el apartado «Linked data» de la referencia citada, ya que es ahí donde se publicará la verificación formal.